Heliyon 6 (2020) e04714

Contents lists available at ScienceDirect

Heliyon

journal homepage: www.cell.com/heliyon

Research article

Information privacy behavior in the use of Facebook apps: A personality-based vulnerability assessment

Karl van der Schyff [a,*], Stephen Flowerday [a], Paul Benjamin Lowry [b]

[a] Department of Information Systems, Rhodes University, Grahamstown, South Africa
[b] Pamplin College of Business, Virginia Tech, Blacksburg, VA, 24061, United States

ARTICLE INFO

Keywords:
Facebook apps
Personality traits
Information privacy concerns (IPCs)
Vulnerability
Facebook privacy settings
Path modeling
Interaction analysis

ABSTRACT

The unauthorized use of personal information belonging to users of apps integrated with the Facebook platform affects millions of users. Crucially, although privacy concerns and awareness have increased, the use of these apps, and related privacy behaviors, remain largely unchanged. Given that such privacy behaviors are likely influenced by individuals' personality traits, it is imperative to better understand which personality traits make individuals more vulnerable to such unauthorized uses. We build on a recontextualized version of the *theory of planned behavior* (TPB) to evaluate the influence of the Big Five personality traits on attitudes toward Facebook privacy settings, social norms, and information privacy concerns (IPCs)—all within the context of Facebook app use. To evaluate this study's model, we analyzed 576 survey responses by way of partial least squares path modeling. Results indicate that highly extraverted individuals are particularly vulnerable to privacy violations (e.g., unauthorized use of personal information) because of their negative attitudes toward Facebook privacy settings. Our post hoc analysis uncovered interesting combinations of personality traits that make individuals particularly vulnerable to the unauthorized use of app-based information. In particular, the combination of extraversion and conscientiousness had a negative effect on individuals' attitude toward privacy settings. We also found a significant negative relationship between *IPCs* and *intention to use Facebook apps*. Finally, we found a positive relationship between social norms and intentions. Taken together, these results infer that individuals are likely to be influenced by their peers in the use of Facebook apps but that their intentions to use these apps declines as privacy concerns increase.

1. Introduction

Despite recent privacy incidents (e.g., Cambridge Analytica), the use of Facebook remains a popular pastime for many users (Acopio and Bance, 2016; Hatzithomas et al., 2017). Importantly, this is mirrored in the use of Facebook Apps[1] which by default harvest a plethora of personal information, including a user's age, gender, and email address (to name but a few) (Pultier et al., 2016). This is particularly evident in the case of Cambridge Analytica where a Facebook app was used to harvest the personality traits of millions of users (Pegg and Cadwalladr, 2018). Referred to as "persuadables" Cambridge Analytica used the harvested personality-based dataset to infer which individuals are more vulnerable to certain Facebook-based stimuli (Amer and Noujaim, 2019). Together, the selected stimuli and harvested Facebook profile information, allowed for detailed voter profiling to take place. Given that the users of Facebook apps are able to control the information they share by making adequate use of privacy settings (Bartsch and Dienlin, 2016; Fiesler et al., 2017), this article performs a similar vulnerability assessment. However, instead of investigating the behavioral influence of stimuli, we investigate the influence of personality traits on Facebook privacy behavior in an attempt to determine which traits are most vulnerable to privacy violations. More specifically, to what extent an individual's personality traits influence their intended use of Facebook apps as a function of their attitude towards privacy settings, social influence, and concerns about information privacy. In this regard we posit that if certain personality traits are particularly negative in their attitude towards information privacy (e.g., avoids using privacy settings), easily influenced, and not concerned, their profile information is more likely to be harvested by

* Corresponding author.
E-mail address: k.vanderschyff@ru.ac.za (K. van der Schyff).

[1] In the context of this study, the term Facebook apps refers to both Facebook-authored apps (e.g., WhatsApp) and third-party apps that allow the use of Facebook credentials (e.g., Spotify and Pinterest). In other words, those apps that are integrated with the Facebook platform.

https://doi.org/10.1016/j.heliyon.2020.e04714
Received 13 July 2020; Received in revised form 6 August 2020; Accepted 10 August 2020

Facebook apps. This, in turn, makes these individuals particularly vulnerability to privacy violations (e.g., unauthorized use of harvested personal information), which we argue can be attributed to their personality traits. This is especially pertinent given that an individual's personality influences their behavior (Ajzen, 2005), in addition to their attitude toward that behavior (Ajzen, 1991). This makes the use of personality traits particularly appealing given the focus on privacy behaviors and initial research which indicates the potential relevance of these traits in an information privacy context (Baek et al., 2014; Ahn et al., 2015; Shropshire et al., 2015). Importantly, the latter behavioral influences subsequently determine the personal information users divulge on their social media profiles and to what extent they make use of Facebook privacy settings to ensure its safety.

This study also builds on the premise that the harvesting of data takes place when users are either unaware of or unconcerned about the privacy of their personal information—in this context, via the use of Facebook apps. Given that Facebook users are seemingly unaware of the extent that such harvesting takes place (Hitlin and Rainie, 2019), our study conceptualizes information privacy concerns (IPCs) as a form of control that replaces perceived behavioral control (PBC), in line with the original *theory of planned behavior* (TPB) (Ajzen, 1991). Additionally, this study investigates the extent to which subjective and descriptive norms (conceptualized as social norms in the research model) influence users' intention to use Facebook apps. As such, this study fundamentally investigates to what extent personality traits influence Facebook users' intention to use Facebook apps as a function of their attitude toward and concerns over information privacy.

Several studies have investigated the influence of IPCs, social norms, and personality traits on intention to use—albeit from different perspectives (Baek et al., 2014; Ahn et al., 2015; Mohammed and Tejay, 2017). For example, some studies have primarily focused on either the Facebook apps themselves (Symeonidis et al., 2018), transactional privacy when using apps (Choi and Land, 2016), privacy risks (Farnden et al., 2015), privacy concerns when using apps (Golbeck and Mauriello, 2016; Wisniewski et al., 2017), or the relationship between users' age and privacy management (Pang and Zhang, 2015; Kezer et al., 2016). The studies that have in fact explored the behavioral influence of information privacy have done so within an organizational context in which social media formed only one component of the larger questionnaire (Parsons et al., 2017). Additionally, studies that have explored the behavioral influence of both personality traits and information security do so by either omitting some of the traits (McCormac et al., 2017) or focusing on populations outside social media (Shropshire et al., 2015; Gratian et al., 2018). We could not find any studies that investigated the influence of both personality traits and IPCs regarding the intention to use secondary apps integrated with the Facebook platform.

Thus, this study contributes to extant theory on two fronts. First, it substitutes the construct IPCs for PBC (as per the original TPB) and proposes that IPCs influence and are influenced by awareness and the acquisition of knowledge. Second, this study contributes to research and practice by indicating which personality traits make users the most vulnerable to the harvesting of personal information via Facebook apps, specifically as a function of respondents' privacy concerns, attitude toward privacy settings, and to what extent they can be influenced by social norms. Although a few studies have investigated the link between the Big Five personality traits and vulnerability, these studies focused either on self-control (Van Wilsem, 2013; Pratt et al., 2014), cyberbullying (Zhou et al., 2018; Balakrishnan et al., 2019, 2020), or cybercrime in general (Van De Weijer and Leukfeldt, 2017).

Accordingly, we proceed as follows. We first present the theoretical foundation, motivating the TPB's suitability for our context. Next, we outline the study's methodological approach and develop the hypotheses. The results of the study are then reported, with a focus on the assessment of the measurement model, path model, and post hoc analyses. We conclude with a discussion of specific contributions to research and practice, limitations, and opportunities for future research.

2. Theoretical foundation

To guide the development of the research model and associated hypotheses, we used an adapted version of the TPB as the theoretical foundation. Using the TPB in this manner has been recommended not only by related information privacy studies (Wagner et al., 2018) but also by studies that have highlighted an apparent lack of both privacy behavior and awareness and by perception-based studies grounded in accepted behavioral theory (Van Schaik et al., 2018). In terms of our theoretical approach and later use of the TPB, our study substitutes IPCs for the traditional PBC construct. We made this choice because users' IPCs exert behavioral control to the extent that they influence the intention to use Facebook apps. For example, users who are highly concerned about information privacy are more likely to decide to avoid the use of Facebook apps.

To better explain the role of behavioral control, other researchers have similarly adapted the TPB by replacing PBC with other constructs. For example, in their study of green food adoption, Ham et al. (2015) included the concept of locus of control as part of PBC construct. Karimi et al. (2017) argued that PBC should be viewed as a concept that includes control, that is, control over an intended behavior but not necessarily control in the broader sense, as explained by locus of control. Interestingly, the latter study defined locus of control as an individual difference, modeling its influence on both PBC and attitude toward entrepreneurial intentions—a statistically significant influence in the context of that study. Conversely, Rhodes and Courneya (2003) discussed subdividing PBC by focusing on the concept of self-efficacy and controllability, that is, on whether a behavior is entirely within an individual's control. Unlike more recent research (Ham et al., 2015), Rhodes and Courneya (2003) defined control as a concept distinct from self-efficacy. Chandran and Aleidi (2018) also adapted the TPB, but they used perceived self-efficacy instead of PBC rather than evaluating the influence of a broad range of resources, including technological ones.

Although some theories provide adequate support for the evaluation of information privacy, attitude, awareness, concerns, and behavioral intent, they do not necessarily incorporate social norms. The studies that have in fact evaluated the influence of social norms have done so using different descriptions, such as *social influence* or *social sanctions* (Herath and Rao, 2009; Johnston and Warkentin, 2010; Siponen and Vance, 2010) or have evaluated the constituent elements of social norms (subjective, descriptive, or injunctive norms) separately (Ifinedo, 2014; Safa et al., 2017). Recent studies that have evaluated social norms as a single construct either use it within different disciplines (Emami and Khajeheian, 2019; Esfandiar et al., 2019; Wang, 2019); or only evaluate the components thereof, such as subjective norms (Tsai et al., 2016) or descriptive norms (Verkijika, 2018; Merhi and Ahluwalia, 2019). In terms of users' privacy concerns and information security awareness, Lowry et al. (2011) made use of *social exchange theory* and combined it with the attitudinal aspect of the *theory of reasoned action*, explicitly arguing in favor of actual self-disclosure as opposed to intent. As with the concept of social norms, few studies have explored IPCs by adapting the TPB. Those that have done so have theoretically explored privacy concerns within the context of the TPB (Tsohou et al., 2015) but have excluded either social norms (Safa et al., 2015; Hajli and Lin, 2016) or both attitude and social norms (Humaidi and Balakrishnan, 2015).

Furthermore, those studies that have used attitude, privacy concerns, and social norms have failed to include either some or all of the Big Five personality factors (Flores and Ekstedt, 2016). As such, combination of constructs used in this study's research model is a sound basis for contributing theoretically to behavioral privacy research.

3. Research model and hypotheses

3.1. The influence of personality traits

Given that users' personality traits (specifically the Big Five) typically influence resultant behavior (Ajzen, 2005) and that this has been observed in other information privacy contexts (Baek et al., 2014; Ahn et al., 2015; Gratian et al., 2018), it is vital to explore how this phenomenon applies to each trait within the information privacy context of this study. This is true in terms not only of their core characteristics, as summarized in Table 1, but also of their influence within specific behavioral contexts. For example, it is likely that the exploratory nature and higher cognitive abilities of individuals high in openness enhance their awareness and knowledge of Facebook's information harvesting practices. Johnston et al. (2016) confirmed the behavioral influence of such exploratory tendencies, reporting that individuals high in openness are more likely to commit information security policy violations. Accordingly, one could argue that these individuals' desire to explore (and thus become more aware and concerned) exceeds their fear of the negative privacy consequences of such exploration, if it benefits them. In view of the recently publicized privacy scandals surrounding the unauthorized use of personal information via the use of a Facebook app as well as the heightened awareness such scandals have occasioned, it is plausible that open individuals are indeed concerned about the extent to which their Facebook friends could surveil their personal information. This may prompt further exploration to understand how such harvesting can take place, which further increases their privacy concerns. It is thus possible that these individuals will cultivate a positive attitude toward the use of privacy settings because of their increased concern over the privacy of their personal information (Gerber et al., 2018). Research on the relationship between personality traits and information security awareness messages has provided additional insight into the strength of the inquisitive nature of these individuals. For example, an Australian study (McCormac et al., 2017) reported a significant and positive relationship between openness and information security awareness. Additionally, openness was found to be negatively related to rewards for compliant within the same Australian context. Given the core characteristics presented in Table 1, this is not unexpected, especially because open individuals avoid conforming to social norms.

For example, Lonnqvist and Itkonen (2016) found that individuals high in openness tend to be friends with other open individuals—especially if they share the same values. Because such individuals exhibit nonconformist attitudes, it follows that social groups consisting of mostly open individuals will be less likely to adhere to social norms. This tendency naturally lends itself to Facebook, where such individuals' Facebook friends will likely consist primarily of other "open" individuals. Thus, it is likely that such people will engage in little norm-driven use of Facebook apps. We further argue that because they are unlikely to conform to group or social norms, they will pursue exploration on their own terms. In summary, we hypothesize that:

H1a. Openness is positively related to attitude toward privacy settings.

H1b. Openness is positively related to information privacy concerns.

H1c. Openness is negatively related to social norms.

Moreover, studies have examined the influence of neuroticism. For example, neuroticism has been found to be negatively associated with perceptions of computer self-efficacy (Uffen et al., 2013). This, in turn, may play into the distrustful nature of people with high degrees of neuroticism. Together with their lack of computer self-efficacy, their distrust may lead to further frustration when attempting to use Facebook privacy settings. Evidence suggests that these feelings of frustration are compounded by such individuals' assessment of themselves as ineffective at managing their own security (Peleg et al., 2017). Research has also found that neurotic individuals are disinclined to adopt privacy protective behaviors (Ho et al., 2017).

We further propose that an increase in awareness will translate into an increase in privacy concerns. For example, if an individual were to become aware of the unauthorized use of their personal information (e.g., Cambridge Analytica), it is plausible that this would strengthen privacy concerns. Because evidence suggests that there is a significant relationship between neuroticism and proactive awareness (Gratian et al., 2018) as well as information security awareness (McCormac et al., 2017), we argue that neurotic individuals will be more concerned in this regard (i.e., they are aware and therefore concerned). Notably, we are not referring to general awareness but rather to awareness regarding the privacy of information within the context of Facebook apps—namely, the level of access an app grants to a user's friends' information and vice versa. We also consider the possibility that fear appeals play a role here. For example, research has suggested a behavioral link between fear and privacy concerns (Bansal et al., 2016; Klobas et al., 2019). In this regard, biological psychology suggests a significant relationship between fear-relevant stimuli, neuroticism, and information processing. Here, research has suggested that a neurotic individual will be more likely affected by fear, thus increasing privacy concerns when under low executive load, that is, when the content does not require extensive processing or cognitive effort (Hur et al., 2016). Because it is likely that a neurotic individual's friends will not have to undertake investigative effort to gain access to that individual's information, we argue that the preceding finding related to the influence of fear will likely increase privacy concerns. From a norms perspective, several studies have suggested that neurotic individuals' insecure nature causes them to emphasize the opinions of others in terms of how they should behave (Bansal et al., 2010; Kajzer et al., 2014). Norm-based influences are thus likely to affect these individuals' use of Facebook apps. We therefore hypothesize that:

H2a. Neuroticism is negatively related to attitude toward privacy settings.

H2b. Neuroticism is positively related to IPCs.

H2c. Neuroticism is positively related to social norms.

Like neurotics, individuals high in agreeableness are generally concerned about the well-being of others and sensitive to the influence of fear (Karim et al., 2009). Their fearful nature may explain their positive attitude toward information privacy (Osatuyi, 2015). For example, agreeable individuals may be fearful that their privacy settings could inadvertently leak information about their friends (Koban et al., 2018) or themselves (Shropshire et al., 2015), especially if this has a negative impact on their well-being. Koohikamali et al. (2017) also found that agreeableness, for both females and males, was significantly related to IPCs. Research on LBSs has also found that agreeableness is significantly related to IPCs (Junglas et al., 2008). More recent research has provided further evidence of a significant relationship between agreeableness and IPCs, specifically regarding electronic commerce transactions (Yeh et al., 2018). Significant relationships between agreeableness and social or group norms have been reported in several other studies. For instance, Erevik et al. (2018) found that individuals high in agreeableness are more attentive to the behavior of others in social settings. Similarly, Stavrova and Kokkoris (2019) found that such individuals are particularly attentive to the needs of their social group. Kim and Chock (2017) found that individuals high in agreeableness post more group selfies. It is thus plausible that individuals high in agreeableness are particularly attentive both to what others are doing (e.g., posting selfies) and to the perception of what they ought to do. As such, if the peers or significant others of

more agreeable individuals use Facebook apps, then "agreeable" individuals will most likely use these apps. Thus,

H3a. Agreeableness is positively related to attitude toward privacy settings.

H3b. Agreeableness is positively related to IPCs.

H3c. Agreeableness is positively related to social norms.

Conscientious individuals are cautious and generally risk averse (see Table 1), which makes them less likely to share knowledge (Hao et al., 2019), possibly due to a concern regarding the secondary use of information. Research has indicated that conscientious individuals are likely to use privacy settings to protect personal information, particularly their personal profile (Kuo and Tang, 2013). It is thus likely that the same privacy behavior applies within the context of Facebook apps. Research has also suggested that conscientious individuals are reluctant online users and particularly wary about sharing personal information (Ross et al., 2009). Given the responsible nature of conscientious individuals, they are also likely to be concerned about the level of access their friends' Facebook apps have to their personal information and vice versa (Symeonidis et al., 2018). In support of this finding, Codish and Ravid (2014) found that individuals high in conscientiousness dislike mechanisms that raise awareness of performance-related information (e.g., leader boards). Conscientious individuals perceive such mechanisms as a demotivating factor; we argue that this perception stems from their concern over the increased awareness of their behavior. Evidence in support of this argument is provided by McCormac et al. (2017), who reported a significant positive relationship between conscientiousness and information security awareness. Like those high in agreeableness, these individuals tend to follow accepted norms. They are also less accident prone and abide by the rules (Shropshire et al., 2015). We therefore propose that:

H4a. Conscientiousness is positively related to attitude toward privacy settings.

H4b. Conscientiousness is positively related to IPCs.

H4c. Conscientiousness is positively related to social norms.

As Table 1 shows, extraverts are more inclined to take risks and seek social interaction regardless of other factors. Their proclivity to engage in risky behavior thus makes it more likely that they will consider it unnecessary to check their privacy settings periodically (Pentina et al., 2016) and will thus be less likely to recognize the benefits of privacy settings. Given that these individuals' heightened levels of cortical arousal lead to an increase in the use of stimuli-rich environments (Wilson et al., 2010), such as Facebook, they may view privacy-related behaviors (e.g., configuring privacy settings) as a distracting exercise—that is, as failing to provide stimulation. Additionally, research has identified either a negative relationship between extraversion and privacy concerns (Hin, 2015; Sharma and Jaswal, 2016) or no significant relationship (Junglas et al., 2008; Osatuyi, 2015). It is thus likely that extraverts are less concerned about the privacy of their app-based information than others.

Moreover, from the perspective of group or social norms, extraverts are generally concerned with the views and opinions of others (Devaraj et al., 2008). It is thus likely that these individuals will make use of Facebook apps if peers and significant others are using them. Extraverts also exhibit a strong desire to communicate (Wolfradt and Doll, 2001), which translates to increased use of mobile devices (e.g., smartphones). Because Facebook use takes place mostly on mobile devices (Chen, 2019), extraverts are more likely to intend to use Facebook apps in a communicative manner. Such forms of communication further increase the likelihood that social-group norms will influence these individuals. For example, Kim and Chock (2017) found a significant relationship between individuals high in extraversion and group selfies, suggesting a high likelihood to engage with social groups. This further increases the likelihood of reciprocal communication within social groups, especially considering the significant relationship between extraversion and the number of Facebook status updates (Ong et al., 2011). We therefore hypothesize:

H5a. Extraversion is negatively related to attitude toward privacy settings.

H5b. Extraversion is negatively related to IPCs.

H5c. Extraversion is positively related to social norms.

3.2. Attitude toward privacy settings

Within the context of this study, *attitude* is defined as an individual's propensity to either positively or negatively evaluate another individual, situation, or behavior (Ajzen, 2005). An individual may have a positive or negative attitude toward the use of Facebook apps for any number of reasons—one being the influence of their personality traits. Notwithstanding such influences, an individual's attitude alone also drives their intention to enact specific behaviors (Kim and Hunter, 1993). In this study, the items associated with the construct *attitude toward privacy settings* evaluate respondents' attitudes toward privacy settings. The premise is that once information is disclosed (via Facebook apps in our context), Facebook starts harvesting information on the user's behavior and in doing so increases their vulnerability to privacy violations. Thus, if individuals form a negative attitude toward information harvesting, they may be more inclined to use privacy settings and therefore more likely to use Facebook apps.

Table 1. Summary of personality trait characteristics.

Traits	Characteristics (when high)	Characteristics (when low)	Sources
Openness	Inquisitive, intellectual, creative, loves exploration, embraces new technology and experiences, higher cognitive abilities, nonconformist, open to risky behavior.	Satisfied with the mundane, conservative, avoids uncertainty and change, supports the status quo.	Skues et al. (2012); Lane and Manner (2011); Xu et al. (2016); Costa and McCrae (1992); Pentina et al. (2016); McCormac et al. (2017); Shropshire et al. (2015); Johnston et al. (2016); Barrick et al. (2001)
Conscientiousness	Organized, responsible, performance-driven, thorough, conformist, cautious about self-disclosure, responsible, follows norms.	Disorganized, careless, weak willed, tends to be irresponsible, disregards norms.	
Extraversion	Needs stimulation, sociable, energetic, engages in risky behavior, influenceable, assertive.	Withdrawn, somber, reserved, conservative.	
Agreeableness	Self-conscious, influenceable, cooperative, nurturing, trusting, friendly, respectful of others' feelings and beliefs.	Ruthless, suspicious, uncooperative, unfriendly, not attentive to others.	
Neuroticism	Emotionally unstable, nervous, sensitive, tends to worry, negative, needs to belong, impulsive, increased amounts of self-disclosure.	Calm, secure, self-satisfied, positive, emotionally stable.	

Several studies involving behavioral studies of technology have provided support for the behavioral influence of attitude. For example, Safa et al. (2015) found that both information security awareness and attitude have a direct and positive influence on the intention of information security professionals to behave securely. Related findings were reported by Blythe et al. (2015), who confirmed the behavioral influence of attitude on the intention of employees to comply with information security policies, albeit qualitatively. Both Ifinedo (2014) and Amankwa et al. (2018) found that attitude displayed the most significant effect size on complying with information security policies. For example, a positive attitude toward security compliance correlated directly to enacting related security behaviors. This confirms the results of earlier studies, which also found a strong correlation between attitude and the intention to adopt secure behaviors in general and information security policies in particular (Hazari et al., 2008; Lee and Kozar, 2005).

Although these compliance studies were empirically situated within organizations, social media studies have showed the same behavioral influence of attitude. For example, several studies have investigated individuals' disclosure of personal information on social media platforms (Chang and Chen, 2014; Hirschprung et al., 2016; Hallam and Zanella, 2017). For example, Chen and Sharma (2015) found that a Facebook user's attitude directly influences their intention to disclose personal information. Such disclosure was found to be particularly significant where Facebook users exhibit positive attitudes toward information disclosure on social media (and toward the use of privacy settings). Given the behavioral influence of attitude, we hypothesize:

H6. Attitude toward privacy settings is positively related to intention to use Facebook apps.

3.3. The influence of social norms

Social norms influence the formation of beliefs that emerge from interactions between members of a social group, community, or organization (Lapinski and Rimal, 2005). For example, social norms act as guiding principles that members follow. Members of social groups take it upon themselves to regulate their own behavior in line with the extant social norms of the larger group. There are, however, occurrences in which the use of Facebook apps affects other users, specifically those in a person's list of friends (Symeonidis et al., 2018). These apps harvest personal information from friends and thus also increases an individual's vulnerability to privacy violations. Consequently, the interplay between the responsible use of certain Facebook apps within a familial environment and the social norms within this social group (i.e., family units) is likely to influence the use of these and similar Facebook apps. However, these individuals may be unaware that certain Facebook apps harvest personal information. To investigate these social norms, this study includes both descriptive and subjective norms—both theoretically (Ham et al., 2015) and in the study's research model. Descriptive norms are defined as behavior that is currently taking place (Ham et al., 2015), whereas subjective norms are defined as an individual's belief as to how others think they should behave (Thompson et al., 2017). For example, if an individual observes his friends or family using a specific Facebook app, it is plausible that the individual will also make use of the app. Consider fitness enthusiasts. They may use Facebook apps to track their fitness levels simply because fitness enthusiasts are expected to use such apps (influence of subjective norms).

The motivation for evaluating the combined influence of subjective and descriptive norms can be further understood by considering the following use of Facebook apps. Facebook-authored apps are presented in the Facebook App Center (Web and mobile version). Frequently, these apps indicate how many other users are using the app, especially when the Facebook app is gamified. Importantly, these apps allow users to comment on, review, share, and view the feeds of other users playing/using similar Facebook apps. These mechanisms favor an experiential approach. For example, users cannot fully appreciate the influence of these mechanisms without using the Facebook App Center. It is, however, precisely the experiential nature of Facebook apps that makes it difficult to ascertain whether the users who are commenting are using the app (descriptive) or just commenting (subjective). Hence, although there are subtle theoretical differences between these behaviors, it is plausible that Facebook users are unlikely to make these distinctions before enacting their intention to either use or avoid Facebook apps. This study is therefore not concerned with the way Facebook users perceive these differences, but with the resultant influence on intended app use as influenced by both subjective and descriptive norms. These, in turn, then determines how vulnerable certain individuals are to privacy violations.

This is especially important within the realm of social media, where subjective norms significantly influence intention to use (Lee et al., 2016), either directly as an influence on behavioral intent or indirectly by influencing PBC, attitude, or both. For example, Kusyanti et al. (2017) found that the more other users trust Facebook, the more likely new or existing users will be to use it, specifically the way Facebook manages the security of users' personal information. Their beliefs about what others deem acceptable thus guide their resultant behavior, even if those beliefs do not reflect the truth. As a case in point, an Australian study found that users generally provided positive responses (i.e., faking good) to questions regarding information security incident response, regardless of the actual circumstances surrounding these incidents (Parsons et al., 2017). Parsons et al. (2017) concluded that respondents' overly positive responses are based on an Australian social norm according to which it is socially unacceptable to report on the behavior of others, regardless of polarity (i.e., good or bad). James et al. (2017) also acknowledged the role of social enhancement, arguing that social media users may develop obsessive behaviors, not because of familial pressures but rather because of their perceptions of how inadequate they are based on comparisons to the information shared by other members. Such feelings of subjective inadequacy further stimulate the obsessive use of social media because these users feel the need to continually engage to overcome these feelings. It thus logically follows that:

H7. Social norms are positively related to intention to use Facebook apps.

3.4. The influence of privacy concerns

Again, instead of using PBC, this study focuses on IPCs. In the TPB, PBC is viewed as perceived self-efficacy in performing a specific behavior (Ajzen, 1991; Chandran and Aleidi, 2018), which is influenced by several factors, in particular knowledge, awareness, and the way knowledge and awareness give rise to concerns. For example, a Facebook user who is made aware of Facebook app-based personal information harvesting (e.g., via media, news, or peers) may thus decide to investigate how such information harvesting affects them due to privacy concerns. Subsequently, new knowledge is acquired, leading to the formation of either a positive or negative attitude toward the use of Facebook apps.

Like the other theoretical concepts discussed thus far, information security awareness influences behavior and is often not measured in terms of how individuals perceive and think about information security (Tsohou et al., 2015; Bartsch and Dienlin, 2016). To address these perceptions, researchers have taken a variety of approaches to understanding how information security awareness, knowledge, and perceptions influence each other. For example, Sundar et al. (2013) found that when participants were made aware of how their personal information could be used in an unauthorized capacity, their intention to disclose personal information was lower than that of participants who were made aware of the benefits of disclosing personal information. As such, resultant privacy concerns further compound participants' inability to make informed privacy decisions, which further increases their vulnerability to privacy violations. For example, Hirschprung et al. (2016) found that when individuals lack the requisite knowledge, they base decisions on speculation. However, the more aware and knowledgeable an individual is, the

more rational these decisions, and related behavior, become. This was confirmed by Van Schaik et al. (2018), who found that Facebook users who are more aware of IPCs were generally satisfied with their privacy settings (i.e., the visibility of their personal information). The latter findings align with those of Miltgen and Peyrat-Guillard (2014), who conducted a similar privacy-based study in several European countries. They found that younger individuals incorrectly believed that their information was safer and more private than it was, whereas the converse was true for older individuals.

Nevertheless, privacy concerns can also influence the disclosure of personal information in unexpected ways. For example, Karwatzki et al. (2017) found that an excessive number of transparent features inhibits individuals from sharing personal information and raises concerns regarding the privacy of personal information. It stands to reason that both knowledge and awareness influence not only information disclosure but also individuals' privacy concerns (Parsons et al., 2017). In instances where information security awareness and knowledge are not attained or are inadequate, individuals may fail to protect their personal information adequately (i.e., they see no reason to be concerned). They may even avoid security behaviors entirely (Bergström, 2015). Given that the use of Facebook apps may result in a reduction of the privacy of personal information (i.e., the app shares part of a user's profile), it is plausible that an individual's IPCs will influence their intention to use these apps. Thus,

H8. IPCs are negatively related to intention to use Facebook apps.

4. Methodology

We adopted a cross-sectional survey methodology to collect primary data (Punch, 2003). This was followed by the application of a statistical technique, namely partial least squares (PLS) path modeling.

4.1. Data collection and screening

After receiving ethical clearance, which included checking for compliance in relation to relevant regulations, the Rhodes University Ethical Standards Committee (RUESC) granted permission for us to collected primary data. As part of this collection process we made use of respondents registered as workers on Amazon Mechanical Turk (AMT). AMT is a crowdsourcing platform that can be used for several purposes, including the recruitment of questionnaire respondents. Several recent studies have reported using AMT in this manner, because it facilitates the creation of a sampling frame that is more representative of the target population (Hirschprung et al., 2016; James et al., 2017; Mamonov and Benbunan-Fich, 2018). Such an approach not only ensures demographic diversity but also avoids the collection of data from students where AMT data is consistently as good and usually better (Lowry et al., 2016; Tsai et al., 2016). In any such AMT study, it is crucial to take basic steps to improve data quality, such as providing clear instructions and disqualifying those who do not follow them, properly filtering eligibility and demographics, and increasing attentiveness (e.g., via attention checks) (Holden et al., 2013; Rouse, 2015; Lowry et al., 2016). We carefully followed these steps in addition to obtaining informed consent from questionnaire respondents.

4.2. Demographics of the sample

The data collection took place in 2019. Although 651 responses (n = 651) were collected, several responses were deemed unsuitable. A suitable response was determined as follows:

- The response had to be complete (i.e., all questions answered),
- Both attention trap questions had to be correctly answered, and
- Respondents had to have spent at least six minutes on questionnaire responses.

Table 2. Sample demographic information (n = 576).

Variable	Frequency	Percentage (%)
Gender		
Male	280	48.6
Female	296	51.4
Age		
18–24	43	7.5
25–34	240	41.7
35–44	154	26.7
45–54	79	13.7
55–64	46	8.0
65–74	14	2.4
Level of education		
No degree or up to high school	228	39.6
Bachelor's degree or equivalent	280	48.6
Master's degree and above	68	11.8

After applying the filter criteria, 576 usable responses (n = 576) remained, and these formed the basis of the multivariate analysis. Table 2 presents the demographic distribution of the sample. Of the respondents, 75.9% were under 45 years of age. Slightly more female (51.4) than male respondents completed the questionnaire, and most of the participants had a bachelor's degree or higher (60.4%). Additionally, most (41.7%) of the respondents fell into the 25–34 age group.

4.3. Measures

Our questionnaire either directly used or adapted items from existing studies (see Table A.1 in Online Appendix A). For example, to evaluate the respondents' personality traits, we used the 44-item Big Five Inventory (BFI) developed by John and Srivastava (1999). In some instances, multiple sources were consulted. Designing questionnaires in this manner is common in the fields of both social psychology (personality component) and behavioral technology research (Judge et al., 2002; Park et al., 2017; Verswijvel et al., 2018; Lee and Borah, 2020).

5. Analysis and results

For model analysis, we applied PLS path modeling using SmartPLS version 3.2.9 (Ringle et al., 2015). We chose PLS because it is especially adept at the validation of mixed models of formative and reflective indicators (and thus more appropriate than covariance-based structural equation modeling for preliminary model building) and ideal for large models (Chin et al., 2003; Gefen and Straub, 2005; Hair et al., 2019; Lowry and Gaskin, 2014).

5.1. Evaluating the measurement model

As a first step toward validating the measurement model, the constructs and their associated items were inspected to ascertain whether their factor loadings exceeded 0.50 (James et al., 2017). One item from the openness scale and one from the agreeableness scale were dropped due to an outer loading below 0.50.

To assess convergent validity, we inspected both the magnitude and significance of the outer loadings. Because we had already eliminated loadings below 0.50, the only remaining criterion to check was the significance of the t-statistics. The t-statistic of each item had to be above 1.96 to achieve a 95% confidence level.

The Fornell–Larcker criterion was used to assess discriminant validity. This criterion is used to evaluate whether the square root of the AVE value of each construct is greater than the correlation coefficients between the constructs in the measurement model (Fornell and Larcker, 1981). Table A.2 presents the square root of the AVE value of each

construct (on the diagonal). All these values satisfied the Fornell–Larcker criterion. The cross-loadings were also inspected to ensure that each of the constructs' items loaded the highest on its intended construct (Table A.3). We also inspected the Heterotrait–Monotrait (HTMT) ratio as another means of assessing discriminant validity. All the HTMT ratios were below 1 (Table A.4). Because all the listed validity criteria were satisfied, we concluded that the model was valid from both a convergent and discriminant perspective.

We also assessed the measurement model for the presence of multicollinearity, a vital step when developing PLS-based models (Hair et al., 2019). The variance inflation factor values (VIFs) of all the items were below 5.0 (Table A.5), thus eliminating multicollinearity (Hair et al., 2010).

Finally, the reliability of the measurement model was evaluated by calculating the composite reliability (CR) and Cronbach's alpha (CA) of each construct (see Table A.2). Reliability testing ascertains whether a questionnaire will produce consistent results (Cronbach, 1951). Both the CR and CA exceeded the accepted threshold of 0.70, establishing the reliability of the measurement model (Tavakol and Dennick, 2011).

5.2. Evaluating the structural model

Because our data exhibited good construct validity and reliability, we conducted the final path modeling using PLS. We evaluated the model's path coefficients, variance explained (R^2), effect sizes (f^2), and predictive relevance (Q^2). These results are detailed in Table A.6 and summarized in Figure 1.

Overall, the results support 10 of the 18 hypotheses and account for 35.7% of the variance (R^2) in the dependent variable (*intention to use Facebook apps*). Based on the bootstrapped (5,000 subsamples) significance tests, *openness* had a significant positive influence on *IPCs* ($\beta = 0.260$, $p < 0.01$) and *attitude toward privacy settings* ($\beta = 0.110$, $p < 0.05$). These results provide support for H1a and H1b but not H1c. *Neuroticism* significantly influenced *IPCs* ($\beta = 0.146$, $p < 0.05$) but not *attitude toward privacy settings* and *social norms*. These results suggest that although neurotic individuals harbor privacy concerns, such concerns do not necessarily lead to the belief that privacy settings are useful (support for H2b, but not H2a and H2c). *Agreeableness* significantly influenced *attitude toward privacy settings* ($\beta = 0.141$, $p < 0.01$) but not *IPCs* and *social norms* (support for H3a, but not H3b and H3c).

Conscientiousness significantly influenced both *attitude toward privacy settings* ($\beta = 0.215$, $p < 0.01$) and *IPCs* ($\beta = 0.183$, $p < 0.01$), supporting H4a and H4b. However, no significant influence was observed between *conscientiousness* and *social norms* (no support for H4c). *Extraversion* was found to significantly influence *attitude toward privacy settings* ($\beta = -0.140$, $p < 0.01$) and *social norms* ($\beta = 0.238$, $p < 0.01$) but not *IPCs* (support for H5a and H5c, but not H5b). Additionally, respondents' attitude toward privacy settings did not significantly influence their intention to use Facebook apps (no support for H6). This may suggest that the perceived benefit of using these settings does not influence intention to use (i.e., their use is of no consequence). Conversely, *social norms* exerted a significant positive influence on *intention to use Facebook apps* ($\beta = 0.518$, $p < 0.01$), thus providing support for H7. *IPCs* exerted a significant negative influence ($\beta = -0.128$, $p < 0.01$) on *intention to use Facebook apps* (support for H8). That is, the more concerned individuals are about the privacy of their personal information, the less they intend to use Facebook apps.

Additionally, we assessed the relative impact of each independent variable by inspecting its effect sizes as derived from the standardized Pearson correlations and interpreted in terms of Cohen's guidelines for r (not to be confused with Cohen's d). Of all the latent constructs, *social norms* exhibited the largest effect size (0.535) [large positive effect] on *intention to use Facebook apps*; followed by *IPCs* (-0.196) [small-to-medium negative effect], and finally, extraversion (0.190) [small-to-medium positive effect]. The construct *attitude toward privacy settings* had a trivial effect on *intention to use Facebook apps* (Cohen, 1988).

Finally, we assessed the predictive relevance of the model's endogenous constructs by calculating Stone–Geisser's Q^2 (Stone, 1974; Geisser and Eddy, 1979). Stone–Geisser's Q^2 was 0.233 for *intention to use Facebook apps*, 0.062 for *attitude toward privacy settings*, 0.027 for *social norms*, and 0.074 for *IPCs*. Hence, the model exhibits reasonable predictive relevance (Hair et al., 2017; Vinzi et al., 2010). Last, we evaluated the influence of several control variables. Gender ($\beta = 0.232$, $p < 0.01$) and education ($\beta = 0.042$, $p < 0.01$) were significantly associated with *intention to use Facebook apps*. Together, the results presented in the Online Appendix and Figure 1 provide evidence that the model is structurally sound.

Table 3. Post hoc analysis results, *** at p < 0.01, ** at p < 0.05, ns = not significant.

Interaction terms	Interaction effects model
EXT * OPEN → APS	-0.167*** ($t = 4.159$)
R^2 (APS)	0.125
Effect size (f^2)	0.033 (small)
EXT * AGR → APS	-0.164*** ($t = 4.383$)
R^2 (APS)	0.126
Effect size (f^2)	0.032 (small)
EXT * CON → APS	-0.205*** ($t = 5.409$)
R^2 (APS)	0.134
Effect size (f^2)	0.043 (small)
CON * OPEN → APS	0.151^{ns} ($t = 0.653$)
AGR * OPEN → APS	0.111^{ns} ($t = 0.750$)
CON * AGR → APS	0.036^{ns} ($t = 0.377$)
CON * OPEN → IPC	0.117^{ns} ($t = 0.701$)
NEU * OPEN → IPC	-0.194^{ns} ($t = 0.963$)
CON * NEU → IPC	-0.050^{ns} ($t = 0.383$)
EXT * OPEN → SN	-0.125^{ns} ($t = 1.526$)
IPC * SN → IUFA	-0.025^{ns} ($t = 0.248$)

5.3. Post hoc interaction analysis

We also conducted a post hoc analysis by adding interaction terms (cross-multiplication of exogenous variables) for several of the personality traits that loaded significantly onto *attitude toward privacy settings*, *social norms*, and *IPCs*. For example, to assess the interaction effects relating to *attitude toward privacy settings* and *IPCs*, we added the interaction terms presented in Table 3.

The results illustrated in Figure 2 suggest that the negative relationship between *extraversion* and *attitude toward privacy settings* is strongest when individuals are high in both extraversion and openness.

Similarly, as Figure 3 illustrates, only individuals high in both extraversion and conscientiousness are likely to exhibit a negative attitude toward privacy settings. This interaction term also accounted for the biggest increase in the explanatory power and effect size in relation to the endogenous construct *attitude toward privacy settings*.

The results of Figure 4 illustrate the interaction between extraversion and agreeableness. As in the other two interaction graphs, a negative attitude toward the use of privacy settings is observed when an individual is high in both personality traits.

6. Discussion

The objective of this study was to investigate the behavioral influence of personality traits on Facebook privacy behavior, specifically their influence on the intention to use Facebook apps as opposed to general social networking use. The construct of *attitude toward privacy settings* was conceptualized as an individual's perception of the usefulness of these settings. By contrast, *IPCs* was conceptualized as how users perceive that Facebook apps are likely to collect personal information, either directly or via Facebook friends.

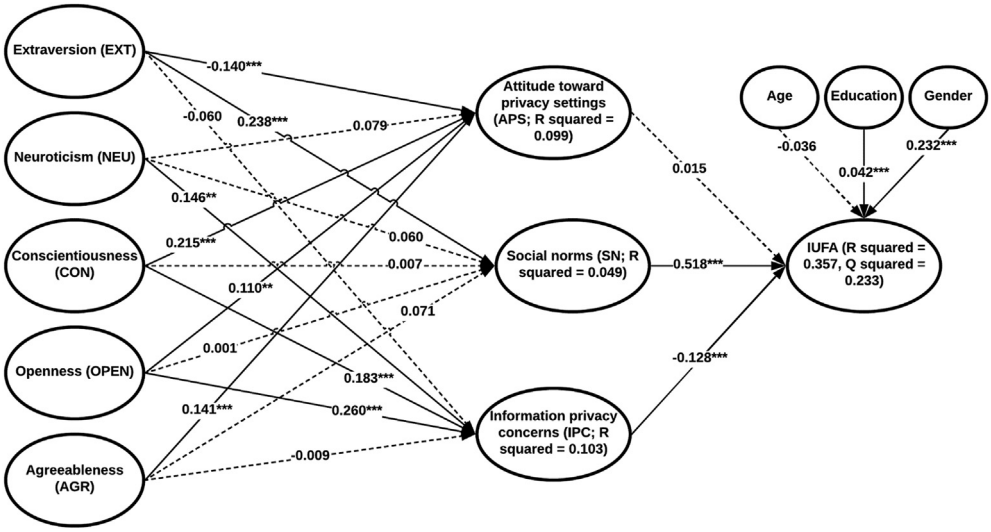

Figure 1. The personality-based Facebook apps privacy model.

The results indicate the absence of a significant relationship between an individual's *attitude toward privacy settings* and their *intention to use Facebook apps*. Additionally, *social norms* were found to positively influence the intention to use Facebook apps. That is, individuals are significantly influenced by their peers when it comes to the intention to use Facebook apps. Additionally, *IPCs* was found to negatively influence the intention to use Facebook apps, which indicates that the intention to use Facebook apps will decrease as privacy concerns increase.

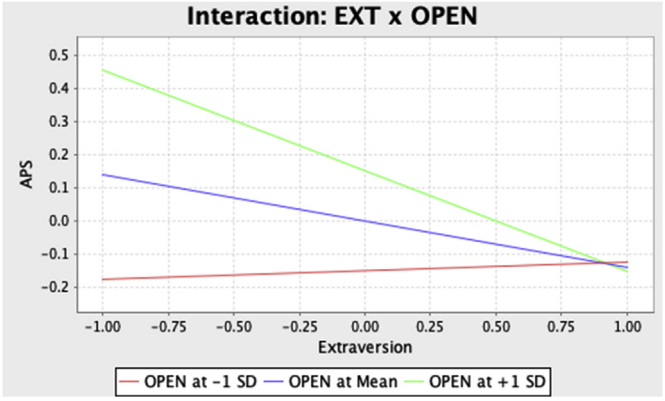

Figure 2. Interaction between extraversion and openness on attitude.

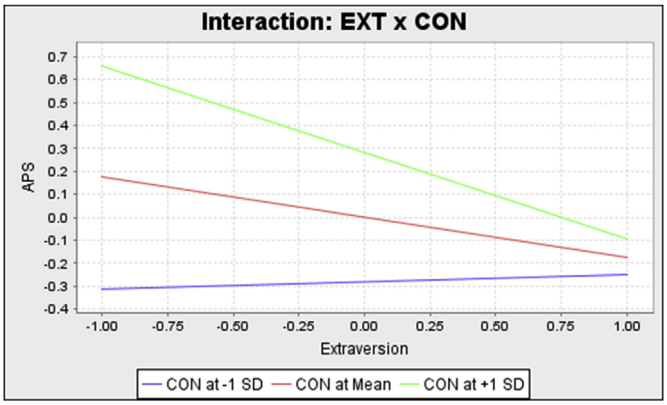

Figure 3. Interaction between extraversion and conscientiousness on attitude.

From a personality perspective, we found that individuals high in extraversion display a negative attitude toward Facebook privacy settings in an app-use context. Conversely, the results show that individuals high in either openness, conscientiousness, or agreeableness display positive attitudes toward the use of Facebook privacy settings. Additionally, all the personality traits, except extraversion and agreeableness, were positively related to IPCs. Of all the personality traits, only extraversion was found to be significantly (and positively) related to social norms. Given the increased use of psychological targeting to aid information harvesting (Matz et al., 2020), and extraverts' social nature, the findings have important privacy implications. First, those who are Facebook friends with sociable, and outgoing individuals (core traits of extraverts) should make adequate use of Facebook privacy settings. In other words, given that extraverts have a negative view of privacy settings, those within their list of Facebook friends may inadvertently find themselves within the reach of such psychological targeting. This is particularly important given that several Facebook apps have access to the friends list of app users. As a result, the apps extraverts use may have access to their friends' personal information in a comparable manner to that of the Facebook app at the center of the Cambridge Analytica controversy. Second, the privacy implications of extraverts' norm-driven use of Facebook apps may be compounded by concepts, such as networked privacy. Given that networked privacy defines the situation where individuals can see each other's content based solely on co-owning or co-creating content (even just being in the same physical location), psychological targeting may be further enhanced (Marwick and Boyd, 2014). In turn, this places the personal information of those associated with extraverts at risk of privacy violations (e.g., unauthorized use of personal information).

Our findings support not only a sizeable number of the hypotheses, but also confirms the results of similar information privacy studies focused on Facebook use. In particular, the positive influence of social norms on the intention to use Facebook apps. As such, using the same Facebook apps as one's peers is a key motivator when it comes to intention to use apps, as is the case with Facebook itself. Having said this, because several of the most popular Facebook apps are games, we argue that the strong influence of norm-driven use may be more closely related to competition with peers than to conformity. Such competitiveness in the use of Facebook apps may also explain the nonsignificant influence of attitude on privacy settings. For example, although some Facebook-based games harvest and share pieces of personal information like those collected by other Facebook apps, the addictive nature of games makes it easy for individuals to ignore information privacy matters. Although individuals may view information privacy as important when sharing

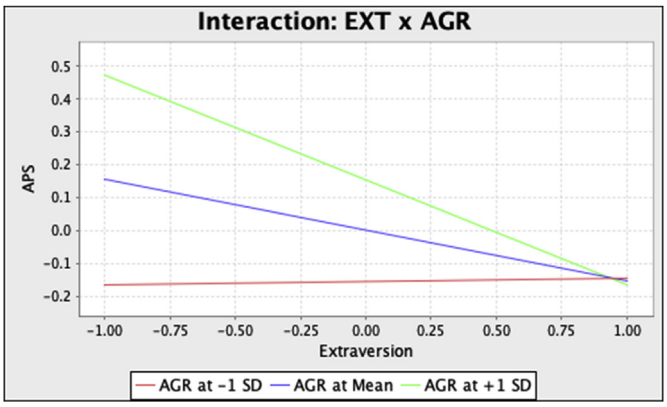

Figure 4. Interaction between extraversion and agreeableness on attitude.

information directly on their Facebook profile or through WhatsApp, they may not be as vigilant when playing a Facebook app game, even though both WhatsApp and the game harvest personal information. This, in turn, increases their vulnerability to privacy violations, as the harvested information is used in an unauthorized manner. We argue that this unauthorized use violates contextual integrity (Nissenbaum, 2009), because Facebook users are not necessarily aware of who receives the harvested information and how this information is reused. Importantly, the resultant use of the information may transcend the initial understanding Facebook users may have had when giving the app consent to use their personal information.

The post hoc analysis also revealed that individuals high in both extraversion and either openness, conscientiousness, or agreeableness display negative attitudes toward privacy settings. This is interesting, considering that taken alone, openness, conscientiousness, and agreeableness are positively related to *attitude toward privacy settings*. Other research has shown a significant positive influence of extraversion on the intention to use or actual use of social media (Amichai-Hamburger and Vinitzky, 2010; Koban et al., 2018). Research has also shown that individuals high in extraversion generally display negative attitudes toward privacy due to their proclivity to participate in risky behavior (Costa and McCrae, 1992; Shropshire et al., 2015; McCormac et al., 2017). That is, they do not think it is necessary to use Facebook privacy settings, at least in an app-use context.

Although all the significant interaction terms in the post hoc analysis contain extraversion as one of the two terms, we find one combination particularly interesting: that of extraversion and conscientiousness. Not only does this personality-trait combination exert the largest effect of all the interaction terms, but it also accounts for greater variance in the latent construct *attitude toward privacy settings*. Paradoxically, several core characteristics of these personality traits are virtually direct opposites of each other yet still result in a significant negative attitude toward privacy settings. For example, highly conscientious individuals are risk averse and cautious when sharing information on social media platforms. Moreover, they are more averse to using social media platforms. In contrast, individuals high in extraversion are open to risky behavior and not as cautious when disclosing information on social media platforms. However, to echo the preceding discussion of Facebook app games, individuals high in both extraversion and conscientiousness are competitive, which makes it likely that they will not see the benefit in using privacy settings when gaming, as long as they can fulfil their desire to compete.

Viewed holistically, several of the personality traits are nonsignificant in their influence on the specified latent constructs. Moreover, those that exert a significant influence do so with small effect. It is therefore likely that there are other predictors that better explain the intention to use Facebook apps in an information privacy context. This is particularly evident when looking at the R^2 value of social norms. From a research perspective, this implies that studies could use other predictors to supplement personality traits when modeling the intention to use Facebook apps as a function of information privacy attitudes and concerns.

7. Limitations and future research

This study has several limitations that point to compelling research opportunities. The most important limitation opens several research opportunities: We found that personality characteristics were not strong predictors of Facebook app use in the context of users' IPCs. Instead, our findings provide further evidence of the consumer "privacy paradox," (Dinev and Hart, 2006; Norberg et al., 2007; Hallam and Zanella, 2017), in which consumers who say they care about their privacy and personal information disclosures often paradoxically abandon such considerations when they actually use technology or social media.

These are particularly troubling findings, because one explanation could be that users of Facebook apps, as well as similar apps, are increasingly conditioned to be apathetic about their privacy. In fact, some researchers have begun to question whether consumer concerns regarding privacy are a historical relics (Dienlin and Trepte, 2015). For example, in a qualitative study, Hargittai and Marwick (2016) found that individuals are generally apathetic about information privacy when using social media. This finding was particularly pronounced for younger individuals who indicated that they had no choice but to use social media, regardless of privacy threats. In extreme cases, the sense of lack of privacy was found to be so severe that participants simply acknowledged that they do not use any privacy settings. The view of many participants was that it was only a matter of time before their personal information would be used in unauthorized manner, suggesting that they view all users as equally vulnerable. This view, regardless of one's use of privacy settings or concerns, is particularly important given the recent unauthorized use of users' Facebook data by Cambridge Analytica. The fact that Hargittai and Marwick's (2016) study predates the Cambridge Analytica scandal makes an even more compelling case that theory should include consideration of the degree to which users are apathetic regarding information privacy in a Facebook app-use context.

From a policy and societal perspective, if this trend continues, the combination of the privacy paradox and consumer apathy places Facebook app developers and similar firms in a strong position to systematically exploit their users' information privacy—regardless of the privacy laws intended to protect consumers. For example, progressive European laws have required much greater disclosures about how companies use private consumer data, along with more informed consent—by providing privacy policies explicitly detailing how consumers' data will be used that users agree to. However, these laws become largely irrelevant if consumers remain apathetic about their privacy and simply skip reading an app's privacy policy and quickly agree to its terms to begin using the app. Ironically, such laws thus may give stronger legal cover to organizations' open exploitation of consumers' private data, because so many consumers willingly hand over such data.

In fact, recent research has shown that this is increasingly pervasive across cultures, because people are driven to satisfy their information and social needs at the expense of privacy concerns (Pentina et al., 2016). Thus, for policy and consumer protection reasons, there are compelling reasons to explore models and methods that could mitigate this gross information privacy imbalance. We likewise concur with researchers and policy makers who advocate for the crucial need to increase consumers' online privacy literacy (Bartsch and Dienlin, 2016). In further examining this literature, we believe a promising direction to address this issue is to better understand and represent just how consumers make privacy-related decisions around "bounded rationality" in a Facebook app setting. Here, researchers could leverage studies on smartphone app-use contexts that has dealt with similar issues, and explained the consumer "privacy paradox" in terms of an extended rational "privacy calculus" model that better considers consumers as operating under

"bounded rationality" (e.g., they have limited cognition, time pressure, limited information, and their decisions are not fully rational, but also emotional) (Keith et al., 2013, 2014, 2015, 2016).

Moreover, we did not focus on the motivations for individuals' use of Facebook apps. Based on other behavioral technology research, we surmise that such motivations are likely mixed and lean toward hedonic motivation and other kinds of intrinsic motivation (e.g., relax, learn, discover) (Posey et al., 2010; Lowry et al., 2015; Shibchurn and Yan, 2015; Church et al., 2017; Mekler et al., 2017; Divine et al., 2019). For example, individuals may use Facebook apps to relax and unwind (e.g., playing Facebook games) as opposed to being productive, which may alter information privacy attitudes and expectations. To address this issue and further investigate the role of norms, researchers could incorporate social psychology theories, such as *self-determination theory*, by investigating the influence of autonomous and controlled motivators (Deci and Ryan, 2008; Rezvani et al., 2017; Mills and Allen, 2020), such as perceived rewards (e.g., enjoyment in the case of games), peer approval, self-esteem, and the individual's ego.

Relatedly, our model and subsequent analysis did not consider all the relationships of the TPB; likewise, it did not consider several extensions of the TPB that would be promising in our context. For example, we did not incorporate the relationships that would typically exist between *social norms* and *attitude toward privacy* as well as *social norms* and *IPCs*. Future research should include similar relationships to understand the influence of norms on privacy attitudes and privacy concerns. It is likely that the addition of these relationships would increase the explanatory power of the constructs *attitude toward privacy settings* and *IPCs*. It is likewise crucial to consider recent TPB extensions and uses that have been effective in consumer privacy paradox settings, such as the posting of selfies (Kim et al., 2016), which are often highly private, and considerations of trust theory extensions (Cheung and To, 2017) for this context.

Researchers should also consider making use of causal and longitudinal data sets, as opposed to the noncausal cross-sectional data set used in this study. This has recently been accomplished, for example, in considering privacy-protective behaviors in smartwatch games (Williams et al., 2019). Such longitudinal approaches can give researchers a clearer idea as to the persistence of the results obtained in this study. This could be particularly useful if mixed motivations are indeed a key factor in this context, because research on mobile app adoption shows that although intrinsic motivations are more important at first, extrinsic motivations become more important over time (McLean, 2018).

Moreover, culture itself has consistently been shown to be a key determinant of privacy perceptions in technology-use contexts (Lowry et al., 2011). First, different countries have different laws and social norms with respect to privacy; for example, Chinese users are consistently less concerned about privacy than Western users (Lowry et al., 2011; Peters et al., 2015). To expand on this, a single study could be conducted in a variety of countries with known differences in views about information privacy. It is likely, for example, that German respondents will have vastly different views about the use of Facebook privacy settings than US respondents. Results from such longitudinal studies would also give a clearer indication of how effective the use of personality traits is in explaining privacy attitudes. For example, the nonsignificant nature of the relationship between *attitude toward privacy settings* and *intention to use privacy settings* may indicate that personality traits are not the best predictor of privacy attitudes. However, this cannot be stated conclusively without further longitudinal work. To further address the nonsignificant nature of attitudes toward privacy settings, future research could include constructs that evaluate concepts such as information privacy control, apathy toward information privacy, privacy fatigue, and Facebook dependency. Individuals who are increasingly dependent on Facebook are likely to exhibit an apathetic attitude toward information privacy, because their motive for using the platform overrides any privacy concerns (Hargittai and Marwick, 2016; Kanat-Maymon et al., 2018).

Another limitation of this study is that it focused only on Facebook apps. To further validate the findings of this study, similar research needs to be conducted on other platforms, such as Google+, where users leverage apps from the Google Play Store. The same applies to users of Apple devices who make use of apps from the App Store. Future research on privacy attitudes and concerns (but not necessarily via apps) could also be conducted on Instagram. The use of Instagram is particularly important, because it is the second most popular social media platform in the United States (Pew Research Center, 2019).

Finally, this study did not incorporate measurement items to assess how socially desirable respondents' answers were. This is especially pertinent given that we found evidence suggesting that some users' intentions may contradict their actual behavior (i.e., their use of apps persists even though they expressed privacy concerns). A recent cross-cultural study dealing with the privacy paradox included such a scale (Peters et al., 2015). It used the classic scale from Crowne and Marlowe (1960). We therefore suggest that researchers include such a social desirability scale in their questionnaires. For example, researchers could include any of the short-form Marlowe–Crowne social desirability scales (Ray, 1984), which would make it possible to exclude responses deemed dishonest (Snyman et al., 2017).

8. Conclusion

This study investigated the influence of personality traits on Facebook privacy behavior. Specifically, to determine which personality traits are most vulnerable to privacy violations, such as the harvesting, and subsequent unauthorized use, of personal information as a function of an individual's attitude towards privacy. In this instance the use of Facebook privacy settings to secure Facebook app-based information. To determine the latter, we recontextualized the TPB by conceptualizing the influence of Facebook users' attitude toward information privacy settings, social norms, and IPCs. Our investigation revealed that only *IPCs* were found to exert a significant negative influence on *intention to use Facebook apps*. Surprisingly, we found attitude towards privacy settings to exert a nonsignificant influence on intention to use Facebook apps, which we conclude may be aligned with the significant influence of social norms within a competitive context. In this regard, we argue that because many Facebook apps are indeed games (or gamified), intended use of apps is possibly driven more by competing with peers than conforming with peers. As a result, and like Facebook, the use of Facebook apps is also subject to social influence. In addition to the statistical analysis, we conclude that there are important privacy implications when considering norm-driven use of Facebook apps. Especially when co-creating/owning content with individuals high in extraversion, whose social and outgoing nature make them (and their Facebook friends) vulnerable to the unauthorized use of harvested personal information. Specifically, through the process of psychological targeting.

Finally, from a personality perspective, and via post hoc analysis, we found that the combined presence of high degrees of *extraversion* and *conscientiousness* exerted the largest negative effect on *attitude toward privacy settings*. We therefore argue that individuals high in both extraversion and conscientiousness are the most vulnerable to information privacy violations, such as the unauthorized use of their Facebook app-based personal information.

Declarations

Author contribution statement

K. Van der Schyff: Conceived and designed the experiments; Performed the experiments; Analyzed and interpreted the data; Wrote the paper.

S. Flowerday, P. B. Lowry: Conceived and designed the experiments; Analyzed and interpreted the data; Contributed reagents, materials, analysis tools or data; Wrote the paper.

Funding statement

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Competing interest statement

The authors declare no conflict of interest.

Additional information

Supplementary content related to this article has been published online at https://doi.org/10.1016/j.heliyon.2020.e04714.

References

Acopio, J., Bance, L., 2016. Personality traits as predictors of Facebook use. Int. J. Psychol. Counsel. 8 (4), 45–52.

Ahn, H., Kwolek, E.A., Bowman, N.D., 2015. Two faces of narcissism on SNS: the distinct effects of vulnerable and grandiose narcissism on SNS privacy control. Comput. Hum. Behav. 45, 375–381.

Ajzen, I., 1991. The theory of planned behavior. Organ. Behav. Hum. Decis. Process. 50 (2), 179–211.

Ajzen, I., 2005. Attitudes, Personality, and Behavior. United Kingdom, LondoMcGraw-Hill Education, London.

Amankwa, E., Loock, M., Kritzinger, E., 2018. Establishing information security policy compliance culture in organizations. Inf. Comput. Secur. 26 (4), 420–436.

Amer, K., Noujaim, J., 2019. The Great Hack [Internet]. Netflix. Available from: https://www.netflix.com/za/title/80117542.

Amichai-Hamburger, Y., Vinitzky, G., 2010. Social network use and personality [Internet] Comput. Hum. Behav. 26 (6), 1289–1295. Available from:

Baek, Y.M., Kim, E.M., Bae, Y., 2014. My privacy is okay, but theirs is endangered: why comparative optimism matters in online privacy concerns. Comput. Hum. Behav. 31, 2414–2419.

Balakrishnan, V., Khan, S., Fernandez, T., Arabnia, H.R., 2019. Cyberbullying detection on twitter using Big five and dark triad features. Pers. Indiv. Differ. 141, 252–257.

Balakrishnan, V., Khan, S., Arabnia, H.R., 2020. Improving cyberbullying detection using Twitter users' psychological features and machine learning. Comput. Secur. 90, 101710.

Bansal, G., Zahedi, F.M., Gefen, D., 2010. The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. Decis. Support Syst. 49 (2), 138–150. Available from:

Bansal, G., Zahedi, F.M., Gefen, D., 2016. Do context and personality matter? Trust and privacy concerns in disclosing private information online. Inf. Manag. 53 (1), 1–21.

Barrick, M.R., Mount, M.K., Judge, T.A., 2001. Personality and performance at the beginning of the new millennium: what do we know and where do we go next? Int. J. Sel. Assess. 9 (1–2), 9–30. Available from:

Bartsch, M., Dienlin, T., 2016. Control your Facebook: an analysis of online privacy literacy [Internet] Comput. Hum. Behav. 56, 147–154. Available from:

Bergström, A., 2015. Online privacy concerns: a broad approach to understanding the concerns of different groups for different uses. Comput. Hum. Behav. 53, 419–426.

Blythe, J.M., Coventry, L., Little, L., 2015. Unpacking security policy compliance: the motivators and barriers of employees' security behaviors. In: Procceedings of the 11th Symposium on Usable Privacy and Security. SOUPS, pp. 103–122.

Chandran, D., Aleidi, A., 2018. Analyzing the influence of gender stereotypes and social norms on female IT entrepreneurial intention in Saudi Arabia. In: Proceedings of the 51st Hawaii International Conference on System Sciences. HICSS, pp. 4133–4140.

Chang, C., Chen, G., 2014. College students' disclosure of location-related information on Facebook. Comput. Hum. Behav. 35, 33–38.

Chen, J., 2019. 15 Facebook Stats Every Marketer Should Know for 2019 [Internet]. Available from: https://sproutsocial.com/insights/facebook-stats-for-marketers/.

Chen, R., Sharma, S.K., 2015. Learning and self-disclosure behavior on social networking sites: the case of Facebook users. Eur. J. Inf. Syst. 24 (1), 93–106.

Cheung, M.F.Y., To, W.M., 2017. The influence of the propensity to trust on mobile users' attitudes toward in-app advertisements: an extension of the theory of planned behavior. Comput. Hum. Behav. 76, 102–111.

Chin, W.W., Marcelin, B.L., Newsted, P.R., 2003. A partial least squares latent variable modeling approach for measuring interaction effects: results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study. Inf. Syst. Res. 14 (2), 127–219.

Choi, B.C.F., Land, L., 2016. The effects of general privacy concerns and transactional privacy concerns on Facebook apps usage. Inf. Manag. 53 (7), 868–877.

Church, E.M., Thambusamy, R., Nemati, H., 2017. Privacy and pleasure: a paradox of the hedonic use of computer-mediated social networks. Comput. Hum. Behav. 77, 121–131.

Codish, D., Ravid, G., 2014. Personality based gamification: how different personalities perceive gamification [Internet]. In: Proceedings of the 22nd European Conference on Information Systems. ECIS, pp. 1–12. Available from: http://aisel.aisnet.org/ecis2014%0Ahttp://aisel.aisnet.org/ecis2014/proceedings/track12/10.

Cohen, J., 1988. Statistical Power Analysis for the Behavioral Sciences. Lawrence Erlbaum Associates, New York.

Costa Jr., P.T., McCrae, R.R., 1992. Four ways five factors are basic. Pers. Indiv. Differ. 13 (6), 653–665.

Cronbach, L.J., 1951. Coefficient alpha and the internal structure of tests. Psychometrika 16 (3), 297–334.

Crowne, D.P., Marlowe, D., 1960. A new scale of social desirability independent of psychopathology. J. Consult. Psychol. 24 (4), 349–354.

Deci, E.L., Ryan, R.M., 2008. Self-determination theory: a macrotheory of human motivation, development, and health. Can. Psychol. 49 (3), 182–185.

Devaraj, S., Easley, R.F., Crant, J.M., 2008. Research note—how does personality matter? Relating the Five-Factor model to technology acceptance and use. Inf. Syst. Res. 19 (1), 93–105.

Dienlin, T., Trepte, S., 2015. Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. Eur. J. Soc. Psychol. 45 (3), 285–297.

Dinev, T., Hart, P., 2006. An extended Privacy Calculus transactions model for e-commerce transactions. Inf. Syst. Res. 17 (1), 61–80.

Divine, A., Watson, P.M., Baker, S., Hall, C.R., 2019. Facebook, relatedness and exercise motivation in university students: a mixed methods investigation. Comput. Hum. Behav. 91, 138–150.

Emami, A., Khajeheian, D., 2019. Social norms and entrepreneurial action: the mediating role of opportunity confidence. Sustainability 11 (1), 158.

Erevik, E.K., Pallesen, S., Andreassen, C.S., Vedaa, Ø., Torsheim, T., 2018. Who is watching user-generated alcohol posts on social media? Addict. Behav. 78, 131–137.

Esfandiar, K., Sharifi-Tehrani, M., Pratt, S., Altinay, L., 2019. Understanding entrepreneurial intentions: a developed integrated structural model approach. J. Bus. Res. 94, 172–182.

Farnden, J., Martini, B., Choo, K.-K.R., 2015. Privacy risks in mobile dating apps. In: Proceedings of the 21st Americas Conference on Information Systems. AMCIS, pp. 1–10.

Fiesler, C., De Choudhury, M., Gilbert, E., Dye, M., Feuston, J.L., Hiruncharoenvate, C., et al., 2017. What (Or Who) Is Public? Privacy Settings and Social Media Content Sharing, pp. 567–580.

Flores, W.R., Ekstedt, M., 2016. Shaping Intention to Resist Social Engineering through Transformational Leadership, Information Security Culture and Awareness, 59. Comput Secur [Internet, pp. 26–44. Available from:

Fornell, C., Larcker, D.F., 1981. Evaluating structural equation models with unobservable variables and measurement error. J. Mar. Res. 18 (1), 39–50.

Gefen, D., Straub, D., 2005. A practical guide to factorial validity using PLS-Graph: tutorial and annotated example. Commun. Assoc. Inf. Syst. 16 (1), 5.

Geisser, S., Eddy, W.F., 1979. A predictive approach to model selection. J. Am. Stat. Assoc. 74 (365), 153–160.

Gerber, N., Gerber, P., Volkamer, M., 2018. Explaining the Privacy Paradox: a systematic review of literature investigating privacy attitude and behavior. Comput. Secur. 77, 226–261.

Golbeck, J., Mauriello, M., 2016. User perception of Facebook app data access: a comparison of methods and privacy concerns. Future Internet 8 (2), 9.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., Ginther, A., 2018. Correlating human traits and cyber security behavior intentions. Comput. Secur. 73, 345–358.

Hair, J.F., Black, W., Babin, B.Y.A., Anderson, R., Tatham, R., 2010. Multivariate Data Analysis: A Global Perspective. Pearson Higher Education, New York.

Hair, J., Hult, T., Ringle, C., Sarstedt, M., 2017. A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM), second ed. Sage, Los Angeles.

Hair, J.F., Risher, J.J., Sarstedt, M., Ringle, C.M., 2019. When to use and how to report the results of PLS-SEM. Eur. Bus. Rev. 31 (1), 2–24.

Hajli, N., Lin, X., 2016. Exploring the security of information sharing on social networking sites: the role of perceived control of information. J. Bus. Ethics 133 (1), 111–123.

Hallam, C., Zanella, G., 2017. Online Self-Disclosure: the Privacy Paradox Explained as a Temporally Discounted Balance between Concerns and Rewards, 68. Comput Human Behav [Internet, pp. 217–227. Available from:

Ham, M., Jeger, M., Ivković, A.F., 2015. The role of subjective norms in forming the intention to purchase green food. Econ. Res. Istraz. 28 (1), 738–748. Available from:

Hao, Q., Yang, W., Shi, Y., 2019. Characterizing the relationship between conscientiousness and knowledge sharing behavior in virtual teams: an interactionist approach. Comput. Hum. Behav. 91, 42–51.

Hargittai, E., Marwick, A., 2016. "What can I really do?" Explaining the Privacy Paradox with online apathy. Int. J. Commun. 10, 3737–3757.

Hatzithomas, L., Misirlis, N., Boutsouki, C., Vlachopoulou, M., 2017. Effects of personality traits on Facebook use. In: 5th International Conference on Contemporary Marketing Issues, pp. 422–436.

Hazari, S., Hargrave, W., Clenney, B., 2008. An empirical investigation of factors influencing information security behavior. J. Inf. Priv. Secur. 4 (4), 3–20.

Herath, T., Rao, H.R., 2009. Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. Decis. Support Syst. 47 (2), 154–165.

Hin, S., 2015. Consumer personality, privacy concerns and usage of location-based services (LBS). J. Bus. Econ. Manag. 3 (10), 1–6.
Hirschprung, R., Toch, E., Bolton, F., Maimon, O., 2016. A methodology for estimating the value of privacy in information disclosure systems. Comput. Hum. Behav. 61, 443–453.
Hitlin, P., Rainie, L., 2019. Facebook Algorithms and Personal Data [Internet]. Pew Research Center. Available from: https://www.pewresearch.org/internet/2019/01/16/facebook-algorithms-and-personal-data/.
Ho, S.S., Lwin, M.O., Yee, A.Z.H., Lee, E.W.J., 2017. Understanding factors associated with Singaporean adolescents' intention to adopt privacy protection behavior using an extended theory of planned behavior. Cyberpsychol. Behav. Soc. Netw. 20 (9), 1–11.
Holden, C.J., Dennie, T., Hicks, A.D., 2013. Assessing the reliability of the M5-120 on amazon's mechanical Turk. Comput. Hum. Behav. 29 (4), 1749–1754.
Humaidi, N., Balakrishnan, V., 2015. Leadership styles and information security compliance behavior: the mediator effect of information security awareness. Int. J. Inf. Educ. Technol. 5 (4), 311.
Hur, J., Iordan, A.D., Berenbaum, H., Dolcos, F., 2016. Emotion–attention interactions in fear conditioning: moderation by executive load, neuroticism, and awareness. Biol. Psychol. 121, 213–220.
Ifinedo, P., 2014. Information systems security policy compliance: an empirical study of the effects of socialisation, influence, and cognition. Inf. Manag. 51 (1), 69–79.
James, T.L., Lowry, P.B., Wallace, L., Warkentin, M., 2017. The effect of belongingness on obsessive-compulsive disorder in the use of online social networks. J. Manag. Inf. Syst. 34 (2), 560–596. Available from:
John, O., Srivastava, S., 1999. The Big Five trait taxonomy: history, measurement, and theoretical perspectives. In: Pervin, L., John, O. (Eds.), Handbook of Personality: Theory and Research, second ed. Guilford, New York, pp. 102–138.
Johnston, A.C., Warkentin, M., 2010. Fear appeals and information security behaviors: an empirical study. MIS Q. 34 (3), 549–566.
Johnston, A.C., Warkentin, M., McBride, M., Carter, L., 2016. Dispositional and situational factors: influences on information security policy violations. Eur. J. Inf. Syst. 25 (3), 231–251.
Judge, T.A., Bono, J.E., Ilies, R., Gerhardt, M.W., 2002. Personality and leadership: a qualitative and quantitative review. J. Appl. Psychol. 87 (4), 765–780.
Junglas, I.A., Johnson, N.A., Spitzmüller, C., 2008. Personality traits and concern for privacy: an empirical study in the context of location-based services. Eur. J. Inf. Syst. 17 (4), 387–402.
Kajzer, M., Darcy, J., Crowell, C.R., Striegel, A., Van Bruggen, D., 2014. An exploratory investigation of message-person congruence in information security awareness campaigns. Comput. Secur. 43, 64–76.
Kanat-Maymon, Y., Almog, L., Cohen, R., Amichai-Hamburger, Y., 2018. Contingent self-worth and Facebook addiction. Comput. Hum. Behav. 88, 227–235.
Karim, N.S.A., Zamzuri, N.H.A., Nor, Y.M., 2009. Exploring the relationship between Internet ethics in university students and the Big Five model of personality. Comput. Educ. 53 (1), 86–93.
Karimi, S., Biemans, H.J.A., Naderi Mahdei, K., Lans, T., Chizari, M., Mulder, M., 2017. Testing the relationship between personality characteristics, contextual factors and entrepreneurial intentions in a developing country. Int. J. Psychol. 52 (3), 227–240.
Karwatzki, S., Dytynko, O., Trenz, M., Veit, D., 2017. Beyond the personalization Privacy Paradox: privacy valuation, transparency features, and service personalization. J. Manag. Inf. Syst. 34 (2), 369–400.
Keith, M.J., Thompson, S.C., Hale, J., Lowry, P.B., Greer, C., 2013. Information disclosure on mobile devices: Re-examining Privacy Calculus with actual user behavior. Int. J. Hum. Comput. Stud. 71 (12), 1163–1173.
Keith, M.J., Evans, C.M., Lowry, P.B., Babb, J.S., 2014. Privacy fatigue: the effect of privacy control complexity on consumer electronic information disclosure. In: 35th International Conference on Information Systems. ICIS, pp. 14–17.
Keith, M.J., Babb, J.S., Lowry, P.B., Furner, C.P., Abdullat, A., 2015. The role of mobile-computing self-efficacy in consumer information disclosure. Inf. Syst. J. 25 (4), 637–667.
Keith, M., Babb, J., Furner, C., Abdullat, A., Lowry, P., 2016. Limited information and quick decisions: consumer privacy calculus for mobile applications. AIS Trans. Hum.-Comput. Interact. 8 (3), 88–130.
Kezer, M., Sevi, B., Cemalcilar, Z., Baruh, L., 2016. Age differences in privacy attitudes, literacy and privacy management on Facebook. Cyberpsychology 10 (1), 1–20.
Kim, J.W., Chock, T.M., 2017. Personality traits and psychological motivations predicting selfie posting behaviors on social networking sites. Telematics Inf. 34 (5), 560–571.
Kim, M.-S., Hunter, J.E., 1993. Relationships among attitudes, behavioral intentions, and behavior: a meta-analysis of past research. Commun. Res. 20 (3), 331–364.
Kim, E., Lee, J.A., Sung, Y., Choi, S.M., 2016. Predicting selfie-posting behavior on social networking sites: an extension of theory of planned behavior. Comput. Hum. Behav. 62, 116–123.
Klobas, J.E., McGill, T., Wang, X., 2019. How perceived security risk affects intention to use smart home devices: a reasoned action explanation. Comput. Secur. 87, 101571.
Koban, K., Stein, J.-P.P., Eckhardt, V., Ohler, P., 2018. Quid pro quo in Web 2.0. Connecting personality traits and Facebook usage intensity to uncivil commenting intentions in public online discussions. Comput. Hum. Behav. 79, 9–18.
Koohikamali, M., Peak, D.A., Prybutok, V.R., 2017. Beyond self-disclosure: disclosure of information about others in social network sites. Comput. Hum. Behav. 69, 29–42.
Kuo, T., Tang, H.L., 2013. Personality's influence on Facebook's privacy settings: a case of college students in Taiwan. In: Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics).
Kusyanti, A., Puspitasari, D.R., Catherina, H.P.A., Sari, Y.A.L., 2017. Information privacy concerns on teens as Facebook users in Indonesia. Procedia Comput. Sci. 124, 632–638.
Lane, W., Manner, C., 2011. The impact of personality traits on smartphone ownership and use. Int. J. Bus. Soc. Sci. 2 (17), 22.
Lapinski, M.K., Rimal, R.N., 2005. An explication of social norms. Commun. Theor. 15 (2), 127–147.
Lee, D.K.L., Borah, P., 2020. Self-presentation on Instagram and friendship development among young adults: a moderated mediation model of media richness, perceived functionality, and openness. Comput. Hum. Behav. 103, 57–66.
Lee, Y., Kozar, K.A., 2005. Investigating factors affecting the adoption of anti-spyware systems. Commun. ACM 48 (8), 72–77.
Lee, S.-Y., Hansen, S.S., Lee, J.K., 2016. What makes us click "like" on Facebook? Examining psychological, technological, and motivational factors on virtual endorsement. Comput. Commun. 73, 332–341.
Lönnqvist, J.-E., Itkonen, J.V.A., 2016. Homogeneity of personal values and personality traits in Facebook social networks. J. Res. Pers. 60, 24–35.
Lowry, P.B., Gaskin, J., 2014. Partial least squares (PLS) structural equation modeling (SEM) for building and testing behavioral causal theory: when to choose it and how to use it. IEEE Trans. Prof. Commun. 57 (2), 123–146.
Lowry, P.B., Cao, J., Everard, A., 2011. Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: the case of instant messaging in two cultures. J. Manag. Inf. Syst. 27 (4), 163–200.
Lowry, P.B., Gaskin, J.E., Moody, G.D., 2015. Proposing the multimotive information systems continuance model (MISC) to better explain end-user system evaluations and continuance intentions. J. Assoc. Inf. Syst. 16 (7), 515–579.
Lowry, P.B., D'Arcy, J., Hammer, B., Moody, G.D., 2016. "Cargo Cult" science in traditional organization and information systems survey research: a case for using nontraditional methods of data collection, including Mechanical Turk and online panels. J. Strat. Inf. Syst. 25 (3), 232–240.
Mamonov, S., Benbunan-Fich, R., 2018. The impact of information security threat awareness on privacy-protective behaviors. Comput. Hum. Behav. 83, 32–44.
Marwick, A.E., Boyd, D., 2014. Networked privacy: how teenagers negotiate context in social media. New Media Soc. 16 (7), 1051–1067.
Matz, S.C., Appel, R., Kosinski, M., 2020. Privacy in the age of psychological targeting. Curr. Opin. Psychol. 31, 116–121.
McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., Pattinson, M., 2017 [Internet]. Individual Differences and Information Security Awareness, 69. Comput Human Behav, pp. 151–156. Available from:
McLean, G., 2018. Examining the determinants and outcomes of mobile app engagement - a longitudinal perspective. Comput. Hum. Behav. 84, 394–403.
Mekler, E.D., Brühlmann, F., Tuch, A.N., Opwis, K., 2017. Towards understanding the effects of individual gamification elements on intrinsic motivation and performance. Comput. Hum. Behav. 71, 525–534.
Merhi, M.I., Ahluwalia, P., 2019. Examining the impact of deterrence factors and norms on resistance to information systems security. Comput. Hum. Behav. 92, 37–46.
Mills, D.J., Allen, J.J., 2020. Self-determination Theory, internet gaming disorder, and the mediating role of self-control. Comput. Hum. Behav. 105, 106209.
Miltgen, C.L., Peyrat-Guillard, D., 2014. Cultural and generational influences on privacy concerns: a qualitative study in seven European countries. Eur. J. Inf. Syst. 23 (2), 103–125. Available from:
Mohammed, Z.A., Tejay, G.P., 2017. Examining privacy concerns and ecommerce adoption in developing countries: the impact of culture in shaping individuals' perceptions toward technology. Comput. Secur. 67, 254–265.
Nissenbaum, H., 2009. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press.
Norberg, P.A., Horne, D.R., Horne, D.A., 2007. The Privacy Paradox: personal information disclosure intentions versus behaviors. J. Consum. Aff. 41 (1), 61–80.
Ong, E.Y.L., Ang, R.P., Ho, J.C.M., Lim, J.C.Y., Goh, D.H., Lee, C.S., et al., 2011. Narcissism, extraversion and adolescents' self-presentation on Facebook. Pers. Indiv. Differ. 50 (2), 180–185.
Osatuyi, B., 2015. Personality traits and information privacy concern on social media platforms. J. Comput. Inf. Syst. 55 (4), 11–19.
Pang, J., Zhang, Y., 2015. A new access control scheme for Facebook-style social networks. Comput. Secur. 54, 44–59.
Park, E.H., Kim, J., Park, Y.S., 2017. The role of information security learning and individual factors in disclosing patients' health information. Comput. Secur. 65, 64–76.
Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., Zwaans, T., 2017. The Human Aspects of Information Security Questionnaire (HAIS-Q): Two Further Validation Studies, 66. Comput Secur [Internet, pp. 40–51. Available from:
Pegg, D., Cadwalladr, C., 2018. US Data Firm Admits Employee Approached Cambridge Analytica: Palantir Confirm Employee 'engaged in a Personal Capacity' with the Company [Internet]. Available from: https://www.theguardian.com/uk-news/2018/mar/28/palantir-employee-cambridge-analytica.
Peleg, S., Vilchinsky, N., Fisher, W.A., Khaskia, A., Mosseri, M., 2017. Personality makes a difference: attachment orientation moderates Theory of Planned Behavior prediction of cardiac medication adherence. J. Pers. 85 (6), 867–879.
Pentina, I., Zhang, L., Bata, H., Chen, Y., 2016. Exploring Privacy Paradox in information-sensitive mobile app adoption: a cross-cultural comparison [Internet] Comput. Hum. Behav. 65, 409–419. Available from:
Peters, A.N., Winschiers-Theophilus, H., Mennecke, B.E., 2015. Cultural influences on Facebook practices: a comparative study of college students in Namibia and the United States. Comput. Hum. Behav. 49, 259–271.

Pew Research Center, 2019. Social media Fact Sheet [Internet]. Available from: https://www.pewinternet.org/fact-sheet/social-media/.
Posey, C., Lowry, P.B., Roberts, T.L., Ellis, T.S., 2010. Proposing the online community self-disclosure model: the case of working professionals in France and the UK who use online communities. Eur. J. Inf. Syst. 19 (2), 181–195.
Pratt, T.C., Turanovic, J.J., Fox, K.A., Wright, K.A., 2014. Self-control and victimization: a meta-analysis. Criminology 52 (1), 87–116.
Pultier, A., Harrand, N., Brandtzaeg, P., 2016. Privacy in mobile Apps [Internet]. Available from: https://tinyurl.com/vk2oftl.
Punch, K., 2003. Survey Research: the Basics. Sage, New Delhi.
Ray, J.J., 1984. The reliability of short social desirability scales. J. Soc. Psychol. 123 (1), 133–134.
Rezvani, A., Khosravi, P., Dong, L., 2017. Motivating users toward continued usage of information systems: self-determination theory perspective. Comput. Hum. Behav. 76, 263–275.
Rhodes, R.E., Courneya, K.S., 2003. Investigating multiple components of attitude, subjective norm, and perceived control: an examination of the Theory of Planned Behaviour in the exercise domain [Internet] Br. J. Soc. Psychol. 42 (1), 129–146. Available from: http://www.ingentaconnect.com/content/bpsoc/bjsp/2003/00000042/00000001/art00008.
Ringle, C., Wende, S., Becker, J., 2015. SmartPLS 3. SmartPLS GmbH, Boenningstedt.
Ross, C., Orr, E.S., Sisic, M., Arseneault, J.M., Simmering, M.G., Orr, R.R., 2009. Personality and motivations associated with Facebook use. Comput. Hum. Behav. 25 (2), 578–586.
Rouse, S.V., 2015. A reliability analysis of Mechanical Turk data. Comput. Hum. Behav. 43, 304–307.
Safa, N.S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N.A., Herawan, T., 2015. Information security conscious care behaviour formation in organizations [Internet] Comput. Secur. 53, 65–78. Available from:
Safa, N.S., Maple, C., Watson, T., Furnell, S., 2017. Information security collaboration formation in organisations. IET Inf. Secur. 12 (3), 238–245.
Sharma, A., Jaswal, I., 2016. Personality correlates of privacy concerns. Indian J. Heal Wellbeing 7 (9), 897–902.
Shibchurn, J., Yan, X., 2015. Information disclosure on social networking sites: an intrinsic-extrinsic motivation perspective. Comput. Hum. Behav. 44, 103–117.
Shropshire, J., Warkentin, M., Sharma, S., 2015 [Internet]. Personality, Attitudes, and Intentions: Predicting Initial Adoption of Information Security Behavior, 49. Comput Secur, pp. 177–191. Available from:
Siponen, M., Vance, A., 2010. Neutralization: new insights into the problem of employee information systems security policy violations. MIS Q. 34 (3), 487–502.
Skues, J.L., Williams, B., Wise, L., 2012. The effects of personality traits, self-esteem, loneliness, and narcissism on Facebook use among university students. Comput. Hum. Behav. 28 (6), 2414–2419.
Snyman, D., Kruger, H.A., Kearney, W.D., 2017. The lemming effect in information security. In: Proceedings of the Human Aspects of Information Security HAISA, pp. 91–103.
Stavrova, O., Kokkoris, M.D., 2019. Struggling to be liked: the prospective effect of trait self-control on social desirability and the moderating role of agreeableness. Int. J. Psychol. 54 (2), 232–236.
Stone, M., 1974. Cross-validatory choice and assessment of statistical predictions. J. R. Stat. Soc. Ser. B 36 (2), 111–133.
Sundar, S.S., Kang, H., Wu, M., Go, E., Zhang, B., 2013. Unlocking the Privacy Paradox: do cognitive heuristics hold the key?. In: Proceedings of the CHI'13 Extended Abstracts on Human Factors in Computing Systems. CHI, pp. 811–816.
Symeonidis, I., Biczók, G., Shirazi, F., Pérez-Solà, C., Schroers, J., Preneel, B., 2018. Collateral damage of Facebook third-party applications: a comprehensive study. Comput. Secur. 77, 179–208.
Tavakol, M., Dennick, R., 2011. Making sense of Cronbach's alpha. Int. J. Med. Educ. 2, 53–55.
Thompson, N., McGill, T.J., Wang, X., 2017. "Security begins at home": determinants of home computer and mobile device security behavior. Comput. Secur. 70, 376–391.
Tsai, H.Y.S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N.J., Cotten, S.R., 2016. Understanding online safety behaviors: a Protection Motivation Theory perspective [Internet] Comput. Secur. 59, 138–150. Available from:
Tsohou, A., Karyda, M., Kokolakis, S., 2015. Analyzing the role of cognitive and cultural biases in the internalization of information security policies: recommendations for information security awareness programs [Internet] Comput. Secur. 52, 128–141. Available from:
Uffen, J., Kaemmerer, N., Breitner, M.H., 2013. Personality traits and cognitive determinants—an empirical investigation of the use of smartphone security measures. J. Inf. Secur. 4 (4), 203–212.
Van De Weijer, S.G.A., Leukfeldt, E.R., 2017. Big Five personality traits of cybercrime victims. Cyberpsychol., Behav. Soc. Netw. 20 (7), 1–6.
Van Schaik, P., Jansen, J., Onibokun, J., Camp, J., Kusev, P., 2018. Security and privacy in online social networking: risk perceptions and precautionary behaviour. Comput. Hum. Behav. 78, 283–297.
Van Wilsem, J., 2013. "Bought it, but never got it" assessing risk factors for online consumer fraud victimization. Eur. Socio Rev. 29 (2), 168–178.
Verkijika, S.F., 2018. Understanding smartphone security behaviors: an extension of the Protection Motivation Theory with anticipated regret. Comput. Secur. 77, 860–870.
Verswijvel, K., Heirman, W., Hardies, K., Walrave, M., 2018. Designing and validating the friendship quality on social network sites questionnaire. Comput. Hum. Behav. 86, 289–298.
Vinzi, V., Chin, W., Henseler, J., Wang, H., 2010. Handbook of Partial Least Squares. Springer, Berlin.
Wagner, A., Wessels, N., Buxmann, P., Krasnova, H., 2018. Putting a price tag on personal information-A literature review. In: Proceedings of the 51st Hawaii International Conference on System Sciences. HICS, pp. 3760–3769.
Wang, E.S.-T., 2019. Effects of brand awareness and social norms on user-perceived cyber privacy risk. Int. J. Electron. Commer. 23 (2), 272–293.
Williams, M., Nurse, J.R.C., Creese, S., 2019. Smartwatch games: encouraging privacy-protective behaviour in a longitudinal study. Comput. Hum. Behav. 99, 38–54.
Wilson, K., Fornasier, S., White, K.M., 2010. Psychological predictors of young adults' use of social networking sites. Cyberpsychol., Behav. Soc. Netw. 13 (2), 173–177.
Wisniewski, P.J., Knijnenburg, B.P., Lipford, H.R., 2017. Making privacy personal: profiling social network users to inform privacy education and nudging. Int. J. Hum. Comput. Stud. 98, 95–108.
Wolfradt, U., Doll, J., 2001. Motives of adolescents to use the Internet as a function of personality traits, personal and social factors. J. Educ. Comput. Res. 24 (1), 13–27.
Xu, R., Frey, R.M., Fleisch, E., Ilic, A., 2016 [Internet]. Understanding the Impact of Personality Traits on mobile App Adoption - Insights from a Large-Scale Field Study, 62. Comput Human Behav, pp. 244–256. Available from:
Yeh, C.H., Wang, Y.S., Lin, S.J., Tseng, T.H., Lin, H.H., Shih, Y.W., et al., 2018. What drives internet users' willingness to provide personal information? Online Inf. Rev. 42 (6), 923–939.
Zhou, Y., Zheng, W., Gao, X., 2018. The relationship between the Big Five and cyberbullying among college students: the mediating effect of moral disengagement. Curr. Psychol. 38 (5), 1162–1173.