A Willingness to Disclose Personal Information for Monetary Reward: A Study of Fitness Tracker Users in Thailand

Original Research

SAGE Open
April-June 2022: 1–15

DOI: 10.1177/21582440221097399
journals.sagepub.com/home/sgo
SAGE

A Willingness to Disclose Personal Information for Monetary Reward: A Study of Fitness Tracker Users in Thailand

Chanchai Phonthanukitithaworn[1] and Carmine Sellitto[2]

Abstract

The paper investigates a person's willingness to reveal personal information for a monetary reward using a model that includes factors reflecting trust belief, risk belief, information type, subjective norm, and privacy concerns. A survey of fitness-tracker users ($N = 504$) using a convenience sampling approach allowed data to be collected. Data analysis used a measurement model to assess construct reliability and validity, with structural equation modeling (SEM) used to test the model's hypotheses. Findings highlight the direct effect of information type and subjective norm as factors that influence privacy. Trust and risk belief associated with information disclosure did not affect privacy concerns nor the willingness to disclose for monetary reward. Subjective norm was the only factor associated with people's willingness to disclose information for monetary reward—highlighting the influence of peer groups and culture on the disclosure process. Notably, subjective norm as a factor that influences information disclosure is seldom reported. The paper contributes to further understanding of factors that influence personal information disclosure when people are offered a monetary incentive. Practical implications include how a reasonable monetary reward can potentially influence disclosure and that leveraging social networks when requesting information may enhance disclosure. Theoretical implications highlight that the modeling of commonly measured risk and trust factors may not hold in certain situations.

Keywords

information, privacy, trust, risk, subjective norm, monetary reward, Thailand, SEM

Introduction

There is an expectation that people will disclose personal information when interacting with websites, social media, and mobile apps (Bauer & Schiffinger, 2016; Degirmenci, 2020; Najjar et al., 2021). Indeed, Lu et al. (2018), highlight the issue of relinquishing personal information online and the subsequent loss of privacy. Privacy refers to an individual's right to control the information disclosed and how it may be used or transmitted to others (Bansal et al., 2016). Privacy might also be viewed as a commodity in the personal information marketplace (Ghosh & Roth, 2015), where consumers place a certain value on privacy when relinquishing data (Malgieri & Clusters, 2018). Furthermore, firms will collect personal information that can be subsequently used to support marketing and sales to customers (Sellitto & Hawking, 2015). Furthermore, access to consumer information is highly desirable for businesses allowing the information to be used to better design products, understand purchase intentions and improve firm revenue (Liang et al., 2019; Morey et al., 2015). From a consumer's perspective, the motivation associated with disclosing personal information will involve reciprocal benefits—such as improved access to services, participating in social media activities, and gaining various rewards (Gómez-Barroso, 2018).

When it comes to relinquishing one's information for monetary incentive, various findings note an enhanced likelihood of disclosure can be motivated by such offerings (Benndorf & Normann,2018; Gómez-Barroso, 2021; Mukherjee et al., 2013; Roth, 2017). Others however, indicate a negative influence—people being less likely to release their details when offered a monetary reward (Lee et al., 2015; Li et al.,

[1]Mahidol University International College, Salaya, Thailand
[2]Victoria University Business School, Melbourne, Australia

Corresponding Author:
Chanchai Phonthanukitithaworn, Business Administration Division, Mahidol University International College, 999 Phutthamonthon IV Road, Salaya, Nakhon Pathom 73170, Thailand.
Email: chanchai.pho@mahidol.ac.th

2010). Furthermore, intrinsic cultural values in regards to revealing personal information can reflect different volitional behavior across groups (Bauer et al., 2018). Indeed, a person's national culture has been shown to influence individuals at the subjective norm level, which shapes their behavioral activities in general (Hofstede et al., 2010; Phonthanukitithaworn & Sellitto, 2016).

The paper proposes and tests a model reflecting a person's willingness to disclose personal information for a monetary incentive. The inclusion of a factor reflecting the willingness to disclose personal information for monetary reward as a dependent variable has not received prominent coverage in the literature. Also included in the proposed model is the construct of subjective norm that reflects an element of national culture influencing information disclosure. Subjective norm has been associated with studies that relate to personal information disclosure per se (Bauer et al., 2018; Heirman et al., 2013; Z. Wang & Liu, 2014)—however, when it comes to subjective norm being associated with the offer of monetary reward for disclosure, seldom research is reported. The target users in the study are Thai nationals who use a fitness-tracking application (app) or dedicated fitness devices to gather personal information about their activities. Thailand is a digital leader in South East Asia with people having a high adoption of smartphone devices, internet use, and acceptance of the digital economy (Deloitte China and Deloitte Southeast Asia, 2021; Google, 2017). Arguably, this level of digital adoption will have enabled Thai citizens to have established a notable personal data footprint—providing an appropriate setting to explore information disclosure.

Literature Review

Gómez-Barroso (2018) indicates that the manner in which consumers reveal their personal information is multidimensional—with no overarching framework that captures all the information disclosure scenarios. However, several salient areas that influenced personal information disclosure included perceived privacy issues, trust in the information-seeking entity, and incentives provided (Liang et al., 2019). Moreover, individual preferences, beliefs, and social norms all influence the behavior of people when revealing personal information (Bauer & Schiffinger, 2016; Gómez-Barroso, 2018). Personal information is highly valued with people being averse to sharing this information, particularly via online sites and third parties (Benndorf & Normann, 2018). Clearly, disclosing one's personal information and the subsequent loss of privacy should not logically occur. However, even when individuals do perceive risks, personal information is still disclosed for various reasons (Mukherjee et al., 2013; Najjar et al., 2021; Prince, 2018; Robinson, 2017)—an observation that has been reported as an information privacy paradox (Barnes, 2006). This privacy paradox is ever evident in the social media space where initial sign-up and ongoing participation compels users to reveal various elements of personal information (Pentina et al., 2016). P. F. Wu (2019), suggests that a trade-off exists between the ongoing level of individual self-disclosure and participation in the social media milieu.

The disclosure of information and associated privacy concerns is considered part of the decision-making process—where influencing factors are evaluated before releasing information (Li et al., 2010; Robinson, 2017). The decision-making process regarding information disclosure in this instance has been referred to as privacy calculus. Privacy calculus reflects the situation where individuals will determine the benefits gained in their decision to relinquish personal information (Dinev & Hart, 2006). Even though individuals may consider the benefits, rewards, and incentives as attractive when asked to disclose information, the evaluated risks associated with loss of privacy may still be too high (Robinson, 2017). Dinev and Hart (2006), suggest that being able to trust the requesting entity and any perceived risks associated with privacy loss were important in deciding whether to reveal information. Notably, there is an ongoing cognitive balance between perceived risks of privacy loss and derived benefits when it comes to disclosure (Buckel & Thiesse, 2013; Dinev & Hart, 2006; Liang et al., 2019).

Perceived risks associated with information disclosure may become a lesser concern as people become familiar with the entity associated with the information exchanged (Robinson, 2017). Trust on the other hand, directly reflects how a person perceives the entity collecting their information to be transparent in initially collecting their data and then appropriately dealing with it after disclosure (Malhotra et al., 2004). Indeed, Hawlitschek et al. (2018) indicate that the trust-sharing economy can be associated with peers, the use of a technology platform, or even a product—entities that will invariably enable sharing. The release of one's personal information for a monetary reward is arguably an example of this trust-sharing proposal where the perceived trust between a person and the information collecting entity can encourage interaction. Bauer et al. (2018), suggests that information disclosure by an individual is more likely to occur if the relationship between the parties is a trustworthy one. Morey et al. (2015), notes a person's trust in a firm is an important factor for consumers when considering whether to relinquish personal information. Contena et al. (2015), found that privacy concerns, control over personal information and trusting social network members influenced information disclosure as part of having a Facebook presence.

Not all information has equal standing when it comes to personal disclosure (Morey et al., 2015)—some information is perceived as more valuable than other information. Malhotra et al. (2004), indicates that information can embody privacy value with information perceived by people to be sensitive influencing the likelihood of disclosure. Lee et al. (2015), indicates that requesting sensitive information intensified an individual's awareness of privacy—any associated benefits or monetary rewards being viewed as a "decoy" by

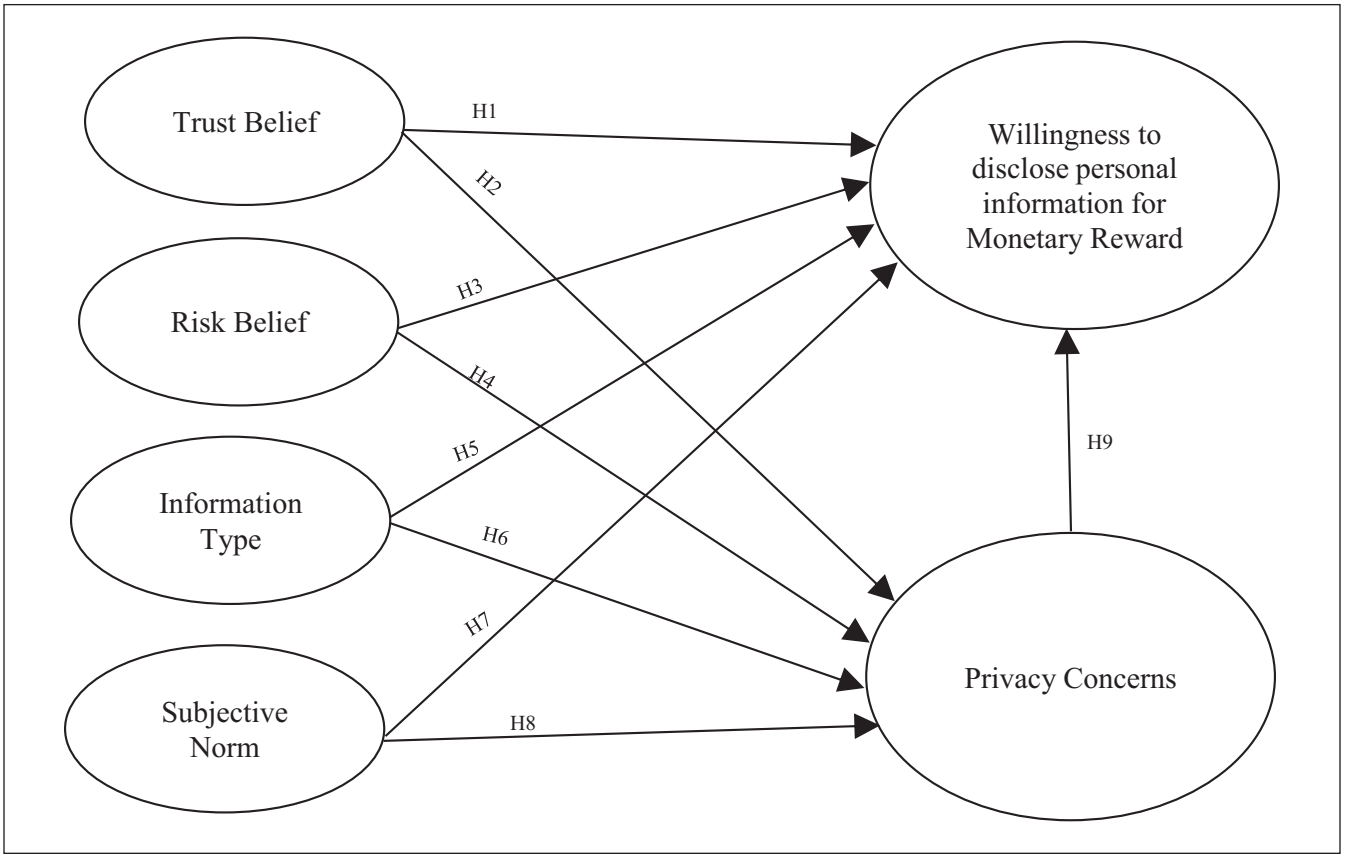

Figure 1. A model for investigating personal information disclosure.

people. Personal information may also embody different formats. It may be text-based, such as providing a person's name, time-based as per social media activity, historical (online reviews), or of a dynamic and visual nature when encapsulated in videos and photographs (Bauer & Schiffinger, 2016; Liang et al., 2019; Morey et al., 2015; Prince, 2018; Shibchurn & Yan, 2014).

Monetary rewards or incentives for personal information disclosure can be viewed as a privacy calculus example of monetary benefits mitigating privacy concerns (Dinev & Hart, 2006; Lu et al., 2018). The literature associated with providing a monetary reward for personal information is only just emerging (Benndorf & Normann, 2018; Ghosh & Roth, 2015; Malgieri & Clusters, 2018; Roth, 2017). Indeed, consumers may be reluctant to divulge their personal information for any monetary incentive (Benndorf & Normann, 2018; Lu et al., 2018). Shibchurn and Yan (2014), suggest that consumers might view the offer of monetary rewards with suspicion—leading people to be selective in what is revealed. Others report that selling personal information has a marketplace with brokers paying consumers for their data (Ghosh & Roth, 2015). Malgieri and Clusters (2018), suggest that personal information has intrinsic commercial value and will be commonly requested by firms as part of the consumer engagement process. Seemingly, some individuals have a propensity to be swayed by a minor monetary gain to reveal personal information that potentially undermines their privacy (Beresford et al., 2012). Monetary cues have been shown to not only positively influence personal information disclosure but also enhance individual willingness to trade off privacy and security in the disclosure process (Mukherjee et al., 2013).

The disclosure of personal information may also be influenced by social subjective norms (Gómez-Barroso, 2018). Subjective norm reflects how the values of others within a peer group directly influence what a person should or should not do with regards to a particular action (Ajzen & Fishbein, 1975). Invariably, subjective norm will be shaped by national culture and intrinsic social beliefs (Phonthanukitithaworn & Sellitto, 2016). The influencing effects of national culture on the disclosure of personal information have been associated with trusting the collecting entity and how that information might be used (Bauer et al., 2018). Robinson (2017), used nationality as an independent variable to investigate the disclosure of personal information in the USA and Estonia. The study reported that the Estonians were far more concerned with privacy and information disclosure than US participants, a finding potentially explained by their national collective identity. National culture has been proposed as playing an important role in moderating the willingness of

Table 1. Hypotheses Used to Test Model Constructs.

Model constructs	Testing hypotheses
Trust belief	H1—There is a positive direct relationship between trust belief and willingness to disclose personal information for monetary reward.
	H2—There is a positive relationship between trust belief and privacy concerns in the disclosure of personal information.
Risk belief	H3—There is a positive direct relationship between risk belief and willingness to disclose personal information for monetary reward.
	H4—There is a positive relationship between risk belief and privacy concerns in the disclosure of personal information.
Information type	H5—There is a positive direct relationship between a given information type and the willingness to disclose personal information for monetary reward.
	H6—There is a positive relationship between a given information type and privacy concerns in the disclosure of personal information.
Subjective norm	H7—There is a positive direct relationship between subjective norm and the willingness to disclose personal information for monetary reward.
	H8—There is a positive relationship between subjective norm and privacy concerns in the disclosure of personal information.
Privacy concern	H9—There is a positive direct relationship between privacy concerns and the willingness to disclose personal information for monetary reward.

people to disclose information when dealing with online sites (K. W. Wu et al., 2012). Bauer and Schiffinger (2016), suggest that a person's cultural background can influence the perceived risk belief as well as their considerations of benefits in the information disclosure decision-making process. Pentina et al. (2016), on the other hand, reported that revealing sensitive information when using mobile apps was not influenced by the cultural background of a person. Nor did the issue of privacy loss influence disclosure.

Research Model and Hypotheses

Based on the previous section's literature, an investigative model (Figure 1) is proposed that includes several dimensions that direct the willingness of individuals to disclose personal information. The model has independent variables that include perceived *trust belief*, perceived *risk belief*, *information type*, and *subjective norm*—constructs that may directly influence an individual's *willingness to disclose personal information for monetary reward. Privacy concerns* will arguably mediate the *willingness to disclose information for monetary reward*. The model's dependent variables include a *willingness to disclose information monetary reward* and *privacy concerns*. Furthermore, Table 1 lists the model's testing hypotheses for each construct proposed. The development of hypotheses occurs in the following section of the paper (while survey items for each construct are noted in the methodology/appendix).

Trust belief. Trust belief relates to the manner in which a person perceives the information-seeking entity as being reliable in protecting their information (Malhotra et al., 2004)—an entity of the trust-economy that may reflect brand product, peer interaction, or technology use that potentially enables sharing, even between strangers (Hawlitschek et al., 2018). Moreover, a person's trust in the information-seeking entity is important given the greater vulnerability of the former in the relationship (Bansal et al., 2016). In the social media environment, trust in other members using the network and the network provider enhances the likelihood of information being revealed (Buckel & Thiesse, 2013). As part of online disclosure activities, a website's perceived reliability and secure data collection practices can address the issue of trust belief (Dinev & Hart, 2006). Lee et al. (2015) suggest that trust belief can be influenced by the presence of a firm's privacy policy, a declaration of how information is to be used and whether the requesting entity has built a relationship with the consumer. The perceptions associated with trust belief also align with consumer privacy concerns—which in turn influences the release of information (K. W. Wu et al., 2012). Clearly, as part of the trust belief construct the protection of disclosed information and the relationship with the requesting entity is important. Hence, in regards to disclosing information gathered via a fitness tracking application, the following hypotheses are proposed:

> H1 There is a positive direct relationship between trust belief and willingness to disclose personal information for monetary reward.
> H2 There is a positive relationship between trust belief and privacy concerns in the disclosure of personal information.

Risk belief. Disclosing personal information online can be influenced by the risk belief a person may have when revealing information (Robinson, 2017). Risk belief reflects

the perception that a greater loss of privacy than expected may occur as a result of disclosing information (Malhotra et al., 2004). Perceived risk belief associated with disclosing information may directly or indirectly result in unexpected financial loss, reputational impact, and psychological damage (Contena et al., 2015; Prince, 2018). Risk belief may be influenced by the relationship established between the information-seeking entity and the disclosing individual—with Robinson (2017) suggesting that when relationships are established, risk perceptions are a lesser concern. Dinev and Hart (2006), suggest there is a dynamic balance between risk beliefs, concerns for privacy loss, and eventual disclosure. Risk belief can also influence the intention to disclose information in the context of considering a monetary reward (Benndorf & Normann, 2018; Mukherjee et al., 2013). Hence, in regards to disclosing information gathered via a fitness tracking application, the following hypotheses are proposed:

H3 There is a positive direct relationship between risk belief and willingness to disclose personal information for monetary reward.
H4 There is a positive relationship between risk belief and privacy concerns in the disclosure of personal information.

Information type. Personal information can have different levels of perceived value when it comes to disclosure (Morey et al., 2015). Information may have commercial value (Elvy, 2017); may be sensitive (Malhotra et al., 2004); or have different privacy levels reflecting a range between most private to least private (Shibchurn & Yan, 2014). The likelihood of people participating in the information disclosure process will tend to be aligned with the people's privacy concerns and the value placed on the information requested (Lee et al., 2015). Prince (2018), indicates identity and demographics data is sensitive information that people may be willing to exchange for an incentive. Benndorf and Normann (2018), suggest that non-identifying information that provides anonymity is likely to be disclosed for an incentive, more so than information that identifies a person. In the social media sphere, people are less likely to self-disclose information associated with their job, location, videos, and photos (Shibchurn & Yan, 2014). Moreover, information will have different perceived value. Hence, we adopt *highly valued* as the given information type in the model. Highly valued information would relate to identifying information such as name, email address, videos, photos, and location. Hence, in regards to disclosing information gathered via a fitness tracking application, the following hypotheses are proposed:

H5 There is a positive direct relationship between a given information type and the willingness to disclose personal information for monetary reward.
H6 There is a positive relationship between a given information type and privacy concerns in the disclosure of personal information.

Subjective norm. Subjective norm relates to how an individual might be influenced by the perceptions of others in regards to whether a particular action should or should not be undertaken (Ajzen & Fishbein, 1975). Subjective norm reflects approval or disapproval activities associated with social interaction (X. Wang & McClung, 2010). The issue of subjective norm is highly reliant on a person's network of peers, family, and friends—networks that represent intrinsic relationships and provide social cues that shape acceptable behavior (Phonthanukitithaworn & Sellitto, 2017). Bauer et al. (2018) proposed that a person's culture had a moderating effect on information disclosure. Notably, people in an individualist society were more likely to consider benefits when disclosing information—compared to those in inclusive collectivist and high power-distance cultures. Z. Wang and Liu (2014), identified the social influence of friends, family, and colleagues as a significant factor in directing people to disclose personal information. Their study of Chinese consumers noted that individuals would be influenced by others in regard to revealing online scenarios. However, social subjective norm may not be a factor when it comes to personal information protection (Chon et al., 2018) For instance, perceived social pressure reflecting the subjective norm feature was found not to be significant when revealing information in exchange for commercial incentives (Heirman et al., 2013). Li et al. (2010), suggest that the association between information disclosure and privacy will differ across nations and cultures—that is, disclosure may be culturally dependent. Hence, in regards to disclosing information gathered via a fitness tracking application, the following hypotheses are proposed:

H7 There is a positive direct relationship between subjective norm and the willingness to disclose personal information for monetary reward.
H8 There is a positive relationship between subjective norm and privacy concerns in the disclosure of personal information.

Privacy concerns. Privacy concerns relate to the ability of a person to control the information disclosed (Contena et al., 2015; Malhotra et al., 2004). In addressing privacy concerns, people need to have an awareness of how information is used by third parties (Lee et al., 2015; Pentina et al., 2016). Contena et al. (2015) indicate that privacy concerns may be associated with how disclosed information might be accessed and/or whether it might be misinterpreted. Hallam and Zanella (2017) examined privacy concerns associated with social networks and noted that privacy was not a significant influence on self-disclosure of personal information—potentially explained the privacy paradox phenomenon. Prince (2018) investigated privacy concerns associated with collecting personal information and noted various issues such as fraudulent selling, sharing, and unauthorized use. Pentina et al. (2016) suggests perceived privacy concerns

associated with information disclosure were influenced by how the information might be shared, its improper use, and being able to correct previous errors. Clearly, privacy concerns affect the willingness of people to disclose personal information. Hence, in regards to disclosing information gathered via a fitness tracking application, the following hypotheses is proposed:

> H9 There is a positive direct relationship between privacy concerns and the willingness to disclose personal information for monetary reward.

Willingness to disclose personal information for monetary reward. A monetary reward can motivate and influence individuals to willingly disclose personal information (Benndorf & Normann, 2018; Lee et al., 2015). Seemingly, monetary reward can be a factor that individuals consider as part of their decision-making process (privacy calculus)—shaping a willingness to reveal personal information (Dinev & Hart, 2006; Lee et al., 2015; Li et al., 2010; Robinson, 2017). Lee et al. (2015), report that many companies collect personal information for marketing purposes and use monetary rewards as an incentive for individuals to disclose details. Monetary rewards as an influence on a person's willingness to disclose information can also be related to hedonic reinforcement, where the provision of a reward increases the likelihood of compliance (Shibchurn & Yan, 2014). Hedonism has been noted as a feature of individualist cultures that are more likely to consider benefits in the information disclosure process (Bauer et al., 2018). Individualist cultures tend to be commonly encountered in western nations, while collectivist nations predominate in Asia (Hofstede et al., 2010; Phonthanukitithaworn & Sellitto, 2016). In regards to the study, trust and risk belief, information type, subjective norm, and privacy concern will arguably influence the willingness of people to release personal information in the scenario where people are offered some monetary reward.

Methodology

Survey Items

The items used to test the proposed model were adapted from previous research associated personal information disclosure (Buckel & Thiesse, 2013; Chon et al., 2018; Contena et al., 2015; Dinev & Hart, 2006; Hallam & Zanella, 2017; Lee et al., 2015; Malhotra et al., 2004; Morey et al., 2015; Pentina et al., 2016; Prince, 2018; Shibchurn & Yan, 2014; Z. Wang & Liu, 2014; X. Wang & McClung, 2010). A 26 item model (see Appendix A) was used to measure the constructs of Trust Belief (TB), Risk Belief (RB), Information Type (IT), Subjective Norm (SN), Privacy Concerns (PC), and the willingness to disclose personal information for Monetary Reward (WD). The items were measured against a seven-point Likert scale with respondents asked to indicate their agreement with item statements that ranged from strongly disagree (1) to strongly agree (7).

A concise survey instrument was developed in English and translated into Thai. Concise surveys have been associated with improved response rates (Sellitto, 2006). Pre-testing of the survey with a cohort of Thai fitness tracking users allowed any anomalies associated with survey wording/instructions to be addressed (Phonthanukitithaworn & Sellitto, 2016). The pre-testing with a group of fitness tracker users also allowed a realistic incentive to be determined which was set at 1,000 baht per month. This was a clearly stated monetary incentive for disclosing personal information as part of the survey. Benndorf and Normann (2018), argued that by clearly indicating the incentive to be received for an information exchange was a definitive and more apt approach to gauging factors associated with disclosure. Furthermore, the monthly reward rationale would have arguably led to a higher cumulative amount for participants, which in turn may have been perceived as meeting a relinquishing threshold—more so than if a single one-off payment had been given.

Sampling and Data Collection

The study's survey used convenience sampling that was undertaken in January/February 2020, resulting in 504 valid responses. For the purpose of this study, the target population included individuals who used a fitness tracker or a smartwatch with an established data tracker history. Fitness tracking apps gather a range of information types which arguably allow the users to determine what might be perceived as personally descriptive and identifying information (highly valued), compared to anonymous or non-identifying information. The data collection technique used in this study was the intercept survey in which potential respondents were intercepted at a location and asked to participate in the research study. Potential respondents were randomly approached by a researcher at various shopping and fitness centers in Bangkok, the capital of Thailand. Bangkok was chosen as the sampling location because the largest pool of fitness tracker and smartwatch users is located in Bangkok (Statista, 2019). The researcher checked to determine whether the potential respondents were appropriate for this study—that is, they were fitness tracker or smartwatch users with an established data tracker history. After fulfilling these criteria, the participant was asked to complete the questionnaire.

These fitness tracking apps ranged from specific devices such as those made by Garmin, Fitbit, and Apple (watch), through to installed mobile-phone apps. A preamble to the survey included a brief scenario statement to provide respondents with the appropriate context for survey questions (see Appendix A). In administering the questionnaire, the researcher clearly related to respondents that the disclosure was for 1,000 baht and that fitness-tracker information was sought. Of the participants in the study, 50.2% ($N=253$)

were male and 49.8% female ($N=251$). The 24 to 41 years age group had the highest ($N=210$) sample representation with other age groupings being 18 to 23 years ($N=105$), 42 to 56 years ($N=139$), and above 57 years ($N=50$).

Data Analysis and Results

This study followed a two-step approach using Structural equation modeling (SEM) analysis as suggested by Byrne (2000) and Hair et al. (2010). The first step examined the reliability and validity of proposed items using a measurement model. The second step tested the hypotheses using a structural model.

Common method variance (CMV) was addressed before analysing the data. CMV can be encountered when a model's variables originate from a similar source or when typically evaluated using similar methodology—with potential errors occurring in the variances associated with these variables. Such errors can lead to an underlying bias when determining the relationships between variables (Podsakoff et al., 2012). Because dependent and independent data were of a perceptual nature and gathered from the same group of participants—any subsequent analysis could be prone to the issue of CMV. Hence, Harman's one-factor analysis was used to check for the influence of CMV and was found to be well below the significant 50% threshold (21.3%)—providing confidence that data analysis was not affected by CMV (see Table B1 in Appendix B).

Measurement Model Assessment

The validity of the model's proposed constructs and items were evaluated simultaneously with confirmatory factor analysis (CFA). The resultant fit statistics [$\chi^2=445.99$ and $df=279$ ($p=.00$)] demonstrated an alignment of the measurement model and the data—in accordance with acceptance levels proposed by Hair et al. (2010). Analysis of the comparative fit index (0.98); the goodness of fit index (0.94); and the normed fit index (0.949) were all above the 0.9 lower acceptance threshold. The root mean square error of approximation (0.03) was below the 0.05 lower limit threshold.

Convergent validity and discriminant validity was undertaken. The measure of convergent validity provides confidence that constructs and composite items are truly related. The measuring of discriminant validity identifies if the proposed constructs are distinctively and not related. The analysis associated with validity is shown in Table 2, with loadings notably greater than 0.70 (T-values significant at .001), Indeed, the calculated AVE and CR exceed the expected lower threshold values of .5 and .7, respectively (Hair et al., 2010)—allowing confidence in claiming convergent validity. Moreover, the relatively high Cronbach α values ($>.700$) indicate that the item scales used are reliable (Tabachnick & Fidell, 2013).

Correlation coefficients and the square root of AVE were compared (Table 3) in order to address the discriminant validity issue. The square root of AVE values are all significantly larger than comparable coefficients providing confidence that discriminant validity has been satisfactorily achieved (Fornell & Larcker, 1981)—that is, the proposed constructs are not related and clearly distinctive.

Hence, confirmation of construct reliability and validity using the measurement model provides confidence in progressing to the subsequent testing of the proposed hypotheses.

Assessment of the Structural Model (Hypothesis Testing)

Figure 2 depicts the structural model analysis of the empirical data to show path diagrams associated with the hypotheses tested and a corresponding standardized parameter estimate. Notably, there was a satisfactory fit aligning the model with the composite data ($\chi^2=445.99$, $df=279$, GFI = 0.94, NFI = 0.95, CFI = 0.98, and RMSEA = 0.03).

Examining model's path relationship associated with privacy concerns—the effect of the information type (H6) and subjective norm (H8) is supported ($\beta=.115$, $p<.05$, $\beta=.195$, $p<.001$ respectively). In other words, information type and subjective norm played a significant role in influencing an individual's privacy concerns to disclose personal data for monetary reward. However, the factors of trust (H2) and risk belief (H4) have not been found to affect an individual's privacy concerns to disclose personal data for monetary reward.

With respect to the effect on willingness to disclose personal data for monetary reward, the factor of subjective norm is the only factor that strongly influences people's willingness to disclose personal data for monetary reward ($\beta=.195$, $p<.001$). Therefore, the H7 is supported. However, the unconfirmed trust belief (H1), risk belief (H3), information type (H5), and privacy concerns (H9) do not support the predicted relation. The direct, indirect, and total effects of the relationships and hypotheses testing are summarized in Table 4.

Discussion and Implications

The paper proposed a five construct model that allowed the investigation of personal information disclosure for a monetary reward. Findings showed that information that was highly valued had a strong direct effect on privacy concerns in the willingness to disclose information. Previous studies report that the request for certain information types can influence privacy concerns (Benndorf & Normann, 2018; Malhotra et al., 2004; Morey et al., 2015; Shibchurn & Yan, 2014). Highly valued information such as images, videos, name, email, and location would identify a person and tend to be reluctantly disclosed. Arguably, the identifying nature of the information requested heightens a person's awareness of privacy loss in the disclosure process. Even though the request for highly valued information influenced privacy

Table 2. Confirmatory Factor Analysis of the Measurement Items.

Construct and measurement items	*M*	*SD*	Standard loading	α	CR	AVE
Trust belief (TB)				.917	.911	.630
I am willing to disclose personal information because. . . .						
TB5 The company has an establish privacy policy	5.45	0.816	0.839			
TB6 The company has a clear objective regarding the usage of my information	5.62	0.847	0.820			
TB7 The company will fulfil promise related to my information	5.80	0.892	0.816			
TB8 The company will handle my information in a competent fashion	5.94	0.831	0.769			
TB9 The company will keep my best interests in mind when dealing with my information	5.77	0.818	0.764			
TB10 The company is transparent in how it will use my data	5.67	0.868	0.751			
Risk belief (RB)				.822	.826	.615
I am willing to disclose personal information because. . . .						
RB11 It has low risk	4.52	0.874	0.775			
RB12 I think the company will not disclose my information to third parties	4.45	0.921	0.849			
RB13 I think there will be no unexpected problems	4.47	0.958	0.818			
Information type (IT)				.873	.855	.544
I am willing to disclose information about my. . . .						
IT21 Location	4.27	1.160	0.720			
IT22 Photos	3.58	1.041	0.819			
IT23 Videos	3.35	1.002	0.826			
IT24 Email address	3.55	0.981	0.757			
IT25 Name and last name	3.47	1.079	0.746			
Subjective norm (SN)				.928	.929	.766
I am willing to disclose my information because. . . .						
SN26 People around me do this	3.90	0.953	0.845			
SN27 Friends do this	4.23	1.108	0.939			
SN28 People who are important to me to this	4.33	1.131	0.895			
SN29 Most people whose opinion I value would think it is fine to disclose my information	4.11	1.116	0.817			
Privacy concern (PC)				.869	.870	.626
I am concerned that my information could. . . .						
PC30 Be misused	3.51	0.868	0.791			
PC31 Be used in a way not foreseen	3.35	0.968	0.829			
PC32 Be shared with others	3.63	0.962	0.756			
PC33 Be misinterpreted	3.56	0.953	0.788			
Willingness to disclose (WD)				.884	.874	.641
WD34 I am willing to disclose my personal information for a monetary reward	3.51	0.883	0.726			
WD35 Offering me a monetary allows me to control how I disclose my information	3.35	0.957	0.711			
WD36 Offering me a monetary will increase the likelihood that I will disclose information in future	3.63	1.057	0.927			
WD37 Offering me a monetary reward has increased my willingness to disclose my information	3.56	1.094	0.898			

Table 3. The Square Root of AVE (in Bold) and Factor Correlation Coefficients.

	PC	TB	RB	IT	SN	WD
PC	**.79**					
TB	.10	**.79**				
RB	.15	.33	**.78**			
IT	.18	.09	.23	**.74**		
SN	.17	.05	.20	.36	**.88**	
WD	.02	.04	.05	.14	.21	**.80**

Note. PC = privacy concern; TB = trust belief; RB = risk belief; IT = information type; SN = subjective norm; WD = willingness to disclose.

concerns, it did not directly influence the willingness to disclose information for a monetary reward. A potential reason for this may relate to people wanting greater compensation for disclosure—more so than what was offered in the study. Benndorf and Normann (2018), noted that people may have high compensation expectations associated with personal information disclosure.

Subjective norm was found to influence the willingness to disclose personal information for monetary reward. It also directly influenced privacy concerns. Subjective norm is associated with the notion that individuals will be influenced by friends, family, and peers on issues that are encountered (Ajzen & Fishbein, 1975). Notably, subjective norm is the only factor that directly influences a willingness to disclose information for monetary reward. Thailand is a collectivist society where relationships and networks between people shape opinions, values, and behavior (Phonthanukitithaworn & Sellitto, 2016). Arguably, people in Thai society value interdependence, solidarity, and loyalty and will tend to be more inclined to check for behavioral trends among peers in shaping their willingness to disclose for a monetary reward. This is consistent with previous work that suggests a collectivist society, in contrast to individualist groups, were less likely to consider benefits in the disclosure process (Bauer et al., 2018). Similarly, privacy concern is potentially influenced by a person's social peers—with peer views also shaping perceptions of privacy loss due to disclosure.

Trust belief is directly related to the perceptions a person has in the information-seeking entity to protect disclosed information (Malhotra et al., 2004). Trust belief did not influence either privacy concerns or the willingness to disclose information for monetary reward. This finding is contrary to other studies that report trust belief as influencing privacy concerns when it comes to personal information disclosure (Bansal et al., 2016; Buckel & Thiesse, 2013; Dinev & Hart, 2006; Malhotra et al., 2004; K. W. Wu et al., 2012). The study sought the disclosure of fitness tracking information. Arguably, people would have experienced information gathering activities when first adopting the fitness tracking app—thus becoming familiar with privacy policy and other data collection issues. This familiarity would likely have built an individual's trust in not only the app, but also app-affiliated brands. Furthermore, the build-up of associated trust over time is likely to also have ameliorated the issue of a person being suspicious of a money-for-information scenario, a scenario which has been noted to restrict the type of personal information that one may reveal (Shibchurn & Yan, 2014). Indeed, the likely ongoing use of the app, may also result in an increased degree of app/brand loyalty—where loyalty in an entity has been noted as further enhancing trust belief (Lee et al., 2015). Furthermore, app use over time would allow people to become aware of how their information might be stored and protected—issues we argue influence trust belief and privacy concerns in the disclosure process (Lee et al., 2015; K. W. Wu et al., 2012).

Risk belief did not influence either privacy concerns or the willingness to disclose personal information for monetary reward. Previous work suggests that a person's view of risk belief relates to the perceptions that a greater loss of privacy than expected occurs because of disclosure (Barnes, 2006; Buckel & Thiesse, 2013; Contena et al., 2015; Malhotra et al., 2004; Prince, 2018; Robinson, 2017). As with trust belief—initial adoption and use of the app, potentially leads to reinforcing a tacit relationship between the app brand (for instance, Garmin) and the fitness tracker user. This type of interaction may ameliorate risk perceptions associated with the loss of privacy, with Robinson (2017) suggesting building relationships with information-seeking entities tends to reduce risk concerns in the information disclosure process. The study found that privacy concerns did not influence the willingness of information disclosure for monetary reward. Given that the constructs of risk belief and trust belief were found to not directly influence privacy concerns, it may be that people felt comfortable about their privacy not being impacted.

Theoretical Implications

The study's approach of modeling monetary reward as a dependent variable in the investigation of a person's willingness to disclose personal information is seldom encountered in the literature. Furthermore, the use of subjective norm as a factor for investigating information disclosure tends to be overlooked. Hence, this investigative approach and the subsequent findings can be argued as contributing to expanding the theoretical literature associated with information disclosure.

Whilst trust and risk belief have been noted as strong influences on privacy concerns in the information disclosure process (Dinev & Hart, 2006; Malhotra et al., 2004; Prince, 2018)—this study did not find this to be the case. This arguably further distinguishes the theoretical contribution of the paper, alerting researchers that these commonly measured influencing factors may not hold in certain situations. We suggest that a familiarity relationship built up over time between the fitness tracker user and the app/brand may have

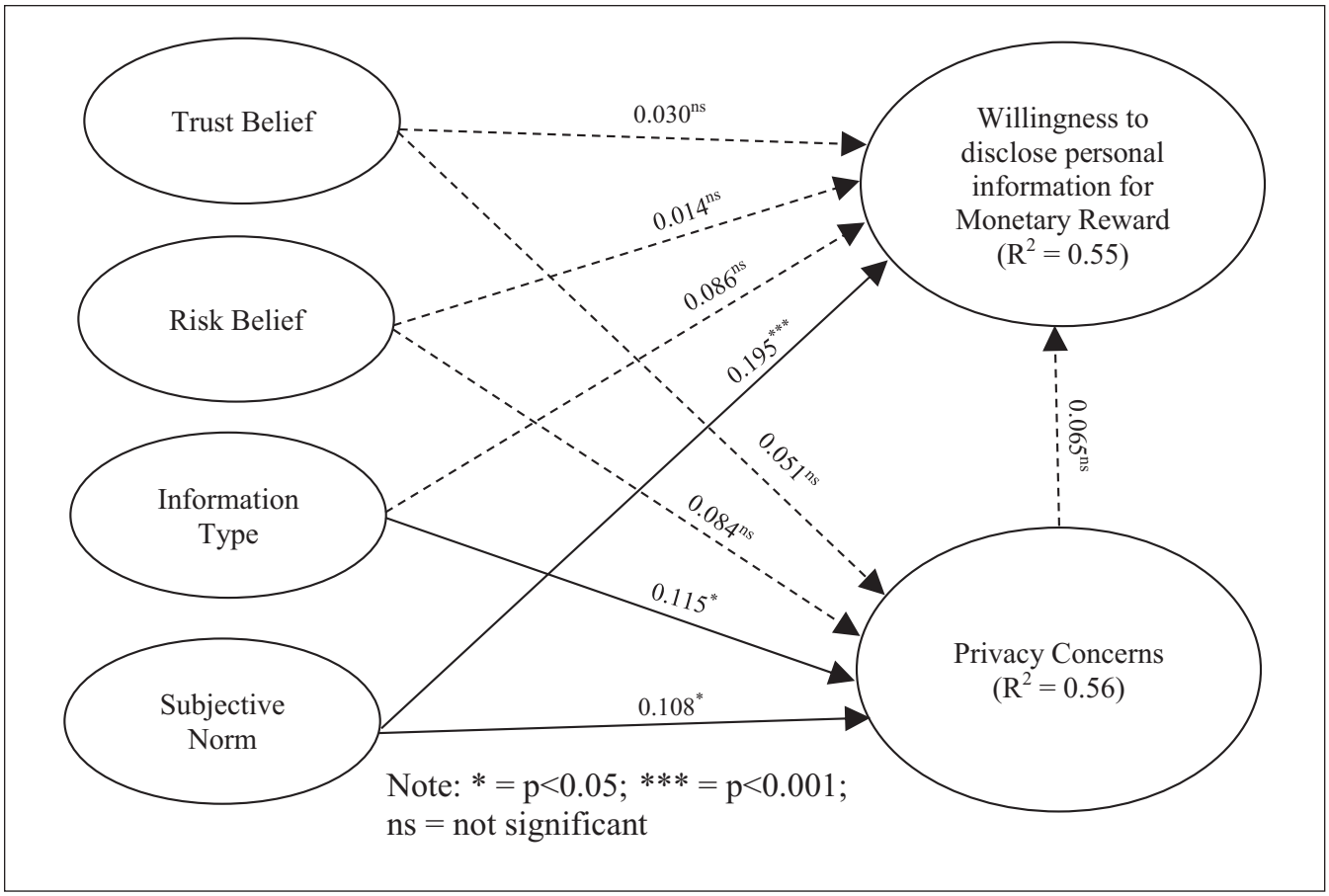

Figure 2. Path analysis and findings (personal information disclosure hypotheses).

Table 4. Direct, Indirect, and Total Effects of the Relationships.

Independent variables	Privacy concerns (PC) ($R^2 = .56$)			Willingness to disclose personal information for monetary reward (WD) ($R^2 = .55$)			Post-hoc mediation analysis results
	Direct effect	Indirect effect	Total effect	Direct effect	Indirect effect	Total effect	
Trust belief	−0.051	—	−0.051ns (H2)	0.030ns (H1)	0.003ns	0.033ns	No effect
Risk belief	−0.084	—	−0.084ns (H4)	−0.014ns (H3)	0.006ns	−0.008ns	No effect
Information type	−0.115*	—	−0.115* (H6)	0.086ns (H5)	0.008ns	0.094ns	Direct effect on PC
Subjective norm	−0.108*	—	−0.108* (H8)	0.195*** (H7)	0.007ns	0.205***	Direct effect on PC and WD
Privacy concern	—	—	—	0.065ns (H9)	—	0.065ns	No effect

Note. ns = not significant.
Standardized coefficients *$p < .05$. ***$p < .001$.

been instrumental in reducing the significance of these two factors. The proposed model per se can also be viewed as a theoretical contribution to be used by other researchers. Even though we found only two influential factors—the same model tested in different situations may be more revealing. For instance, a greater number of factors may be significant in a scenario where a person may not have an understanding or familiarity of the information associated with an often-used app or device (as in this study).

Another important theoretical contribution relates to the significant influence of subjective norm on privacy concerns and willingness to disclose personal information for monetary reward. Seldom are national culture factors investigated in this context—although information disclosure can be culturally dependent (Bauer et al., 2018; Li et al., 2010). The inclusion of subjective norm in the study can be viewed as an important theoretical contribution highlighting the importance of culturally-related factors in explaining findings—particularly in

collectivist and high power distance orientated countries similar to Thailand.

Practical Implications

The study has several important practical implications for organizations that seek personal information from individuals. The significant relationship between information type and privacy concerns implies that even though some incentives are offered in exchange for personal data, people will still be concerned about the type of information requested—especially identifying information such as pictures, video, email location, and name. Furthermore, the request for personal information needs to be balanced with offering a monetary incentive that is perceived as reasonable compensation and one that meets the expectations of the target audience. Invariably, consumer management processes will seek intrinsic personal information through marketing engagement approaches (Malgieri & Clusters, 2018). Hence, any monetary reward should be set at a realist level as might be identified in preliminary investigations of a particular client base. Moreover, organizations might consider regular personal information requests, rather than a one-off event (for instance, monthly disclosure for an agreed period) potentially increasing the likelihood of individuals being more attracted to cumulative rewards. That is, the expectations for disclosure are met as a monetary aggregate over time to potentially address the issue of adequate compensation in reaching a relinquishing threshold (Benndorf & Normann, 2018).

The influence of subjective norm on an individual's privacy concerns and their willingness to disclose personal information for monetary reward highlights the importance of peers, family, and friends in the disclosure process. This is particularly relevant in close-knit integrated collectivist groups where network effects can be leveraged. Organizations would do well to explore these networks when requesting information. For instance, at the fitness-tracker level and contingent on data privacy regulations, operators (not the users) of such devices might even consider directly engaging with known networks of peers, friends, and family members—promoting information sharing rewards to network members that may not be currently partaking in information release/reward. Furthermore, trust and risk belief in the disclosure process was argued as being influenced by ongoing app use and familiarity—potentially reflecting the established tacit relationship and loyalty between a user and app brand. Organizations should be aware that a person's familiarity with a brand or product will potentially reduce the significance these two constructs have when requesting information.

Conclusion and Future Research

The study examined personal information disclosure for monetary reward. Only the culturally-aligned construct of subjective norm directly influenced the willingness to disclose personal information for monetary reward. The factors of trust belief, risk belief, information type, and privacy concerns were not found to influence the willingness to disclose information for a monetary reward. There was a direct effect of information type and subjective norm on privacy concerns. Surprisingly, trust and risk belief was not a significant influence on the willingness to disclose information or people's privacy concerns.

The study was cross-sectional in nature. Future research could examine factors affecting willingness to disclose personal data for monetary reward within specific parameters such as age (for instance Gen X, Y, and Z)—directly comparing the different generational groups. Future work may also involve testing the model in a setting where a reward is a non-monetary type or even not offered at all. The non-offering of a reward potentially will identify neutral settings associated with information disclosure and reflect a baseline scenario that could be compared to a situation when rewards are offered. In the non-monetary reward scenario, the study would potentially uncover if the reward type made a significant influence on information disclosure.

The study was conducted in Thailand which is a strongly collectivist and high power-distance culture with peer opinion influencing all aspects of society (Phonthanukitithaworn & Sellitto, 2017)—an issue that potential may induce Thais to be inclined to relinquish personal information if they see others in society do so, or even if someone influential should request this. Hence, the findings of this study are potentially applicable to collectivist type societies such as Thailand and other countries located in Asia (Hofstede et al., 2010). Notably, we are not able to claim generalization of our work because of this issue. Indeed, future studies may wish to undertake investigations in cross-cultural settings to elucidate the effect of national culture on information disclosure—where a greater number of culturally-based constructs in the model might be used. The adoption of a fitness tracker, like many other consumer products, will potentially be influenced by subjective norm values associated with social and peer interactions. It would be interesting to see if subjective norm identified as influencing fitness-tracker adoption was also a significant factor associated with information release in the same user. This study gauged people's willingness to disclose personal information for monetary reward. While this approach is valuable in understanding the antecedents of willingness, future research could use experimental settings or in-depth interviews to gauge more precisely consumers' actual disclosure behavior.

Limitations

The value of personal information tends to be moderated at the individual level (Mukherjee et al., 2013). Hence, what may be considered to be highly personal for one person, may hold a lesser value for another. These different perceptions of information can be viewed as a limitation in that it may have influenced the response to survey questions. Another limitation is that the fixed monetary reward offered may have been insufficient to induce disclosure for some people whilst seemingly being acceptable for others. The specific focus on fitness tracker users may reflect a group that was comfortable with releasing the information associated with their app and being more trusting

and risk-averse than expected—an issue that seemingly contrasts with individuals knowing that potentially high levels of personal health data were collected by the device.

Appendix A

Scenario

A fitness-tracking firm has approached you to offer a monetary reward for the data that is associated with the app or device you have been using. You are required to disclose personal information as part of the process. The monetary reward is 1,000 Baht per month.

Measurement Items

For each of the questions, please indicate your agreement with the statement on a scale of 1 (strongly disagree) to 7 (strongly disagree).

Constructs and measurement items	Source
Trust belief	Buckel and Thiesse (2013), Dinev and Hart (2006), Lee et al. (2015), and Malhotra et al. (2004)
TB5 I am willing to disclose personal information because I believe the company will have an establish privacy policy	
TB6 I am willing to disclose personal information because I believe the company will have a clear objective regarding the usage of my information	
TB7 I am willing to disclose personal information because I believe the company will fulfil promises related to my information	
TB8 I am willing to disclose personal information because I believe the company will handle my information in a competent fashion	
TB9 I am willing to disclose personal information because I believe the company will keep my best interests in mind when dealing with my information	
TB10 I am willing to disclose personal information because I believe the company will be transparent in how it will use my data	
Risk belief	Buckel and Thiesse (2013), Contena et al. (2015), Dinev and Hart (2006), and Malhotra et al. (2004)
RB11 I am willing to disclose personal information because I believe it has a low risk	
RB12 I am willing to disclose personal information because I believe the company will not disclose my information to third parties	
RB13 I am willing to disclose personal information because I believe there will be no unexpected problems	
Information type	Hallam and Zanella (2017), Malhotra et al. (2004), Morey et al. (2015), Prince (2018), Shibchurn and Yan, (2014), Chon et al. (2018), and Lee et al. (2015)
IT21 I think I am willing to disclose information about my location	
IT22 I think I am willing to disclose information about my photos	
IT23 I think I am willing to disclose information about my videos	
IT24 I think I am willing to disclose information about my email address	
IT25 I think I am willing to disclose information about my name and last name	
Subjective norm	Bauer and Schiffinger (2016), Chon et al. (2018), Phonthanukitithaworn and Sellitto (2017), and X. Wang and McClung (2010)
SN26 I think I am willing to disclose my personal information because people around me do this	
SN27 I think I am willing to disclose my information because my friends do this	
SN28 I think I am willing to disclose my information because people who are important to me do this	
SN29 Most people whose opinion I value would think it is fine to disclose personal information	
Privacy concerns	Buckel and Thiesse (2013), Contena et al. (2015), Dinev and Hart (2006), Hallam and Zanella (2017), Lee et al. (2015), Malhotra et al. (2004), Pentina et al. (2016), and Prince (2018)
PC30 I think I am concerned that my information could be misused	
PC31 I think I am concerned that my information could be used in a way not foreseen	
PC32 I think I am concerned that my information could be shared with others	
PC33 I think I am concerned that my information could be misinterpreted	
Willingness to disclose personal data for monetary reward	Lee et al. (2015), Li et al. (2010), and Prince (2018)
WD34 I think I am willing to disclose my personal information for a monetary reward	
WD35 I think offering me a monetary reward allows me to control how I disclose my information	
WD36 I think offering me a monetary reward will increase the likelihood that I will disclose my information in the future	
WD37 I think offering me a monetary reward has increased my willingness to disclose my information	

Appendix B

Table B1. Total Variance Explained.

	Initial eigenvalues			Extraction sums of squared loadings		
Component	Total	% of variance	Cumulative %	Total	% of variance	Cumulative %
1	5.538	21.301	21.301	5.538	21.301	21.301
2	4.216	16.216	37.517			
3	3.012	11.583	49.101			
4	2.441	9.389	58.490			
5	2.138	8.223	66.713			
6	1.732	6.662	73.375			
7	0.789	3.036	76.410			
8	0.602	2.316	78.726			
9	0.569	2.188	80.914			
10	0.496	1.909	82.824			
11	0.480	1.848	84.671			
12	0.464	1.783	86.454			
13	0.419	1.613	88.067			
14	0.357	1.373	89.440			
15	0.339	1.303	90.743			
16	0.328	1.260	92.003			
17	0.301	1.159	93.162			
18	0.268	1.030	94.192			
19	0.260	1.002	95.194			
20	0.250	0.962	96.156			
21	0.232	0.893	97.050			
22	0.208	0.799	97.848			
23	0.158	0.609	98.458			
24	0.150	0.579	99.036			
25	0.126	0.483	99.520			
26	0.125	0.480	100.000			

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iDs

Chanchai Phonthanukitithaworn https://orcid.org/0000-0001-9639-0936

Carmine Sellitto https://orcid.org/0000-0001-6119-9242

References

Ajzen, I., & Fishbein, M. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research*. Addison-Wesley.

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

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, *11*(9). https://doi.org/10.5210/fm.v11i9.1394

Bauer, C., & Schiffinger, M. (2016). *Perceived risks and benefits of online self-disclosure: Affected by culture? A meta-analysis of cultural differences as moderators of privacy calculus in person-to-crowd settings* [Conference session]. Proceedings of the 24th European Conference on Information Systems, İstanbul, Turkey (pp. 1–19).

Bauer, C., Schiffinger, M., & Strauss, C. (2018). *An open model for researching the role of culture in online self-disclosure* [Conference session]. Proceedings of the 51st Hawaii International Conference on System Sciences, Waikoloa, HI, USA (pp. 3637–3646).

Benndorf, V., & Normann, H. T. (2018). The willingness to sell personal data. *The Scandinavian Journal of Economics*, *120*(4), 1260–1278. https://doi.org/10.1111/sjoe.12247

Beresford, A. R., Kübler, D., & Preibusch, S. (2012). Unwillingness to pay for privacy: A field experiment. *Economic Letters*, *117*(1), 25–27. https://doi.org/10.1016/j.econlet.2012.04.077

Buckel, T., & Thiesse, F. (2013). *Predicting the disclosure of personal information on social networks: an empirical*

investigation [Conference session]. Proceedings of the 11th International Conference on Wirtschaftsinformatik, Leipzig, Germany (pp. 1619–1634).

Byrne, B. M. (2000). *Structural equation modeling with AMOS: Basic concepts, applications, and programming*. Psychology Press.

Chon, B. S., Lee, J. K., Jeong, H., Park, J., & Park, J. (2018). Determinants of the intention to protect personal information among Facebook users. *ETRI Journal*, *40*(1), 146–155. https://doi.org/10.4218/etrij.2017-0082

Contena, B., Loscalzo, Y., & Taddei, S. (2015). Surfing on social network sites: A comprehensive instrument to evaluate online self-disclosure and related attitudes. *Computers in Human Behavior*, *49*, 30–37. https://doi.org/10.1016/j.chb.2015.02.042

Degirmenci, K. (2020). Mobile users' information privacy concerns and the role of app permission requests. *International Journal of Information Management*, *50*, 261–672. https://doi.org/10.1016/j.ijinfomgt.2019.05.010

Deloitte China and Deloitte Southeast Asia. (2021, February). *Emerging digital life in south and southeast asia*. Author. https://journal.isca.org.sg/2021/02/01/emerging-digital-life-in-south-and-southeast-asia/pugpig_index.html

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61–80. https://doi.org/10.1287/isre.1060.0080

Elvy, S. A. (2017). Paying for privacy and the personal data economy. *Columbia Law Review*, *117*(6), 1369–1459.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, *18*(1), 39–50. https://doi.org/10.1177/002224378101800104

Ghosh, A., & Roth, A. (2015). Selling privacy at auction. *Games and Economic Behavior*, *91*, 334–346. https://doi.org/10.1016/j.geb.2013.06.013

Gómez-Barroso, J. L. (2018). Experiments on personal information disclosure: Past and future avenues. *Telematics and Informatics*, *35*(5), 1473–1490. https://doi.org/10.1016/j.tele.2018.03.017

Gómez-Barroso, J. L. (2021). Feel free to use my personal data: An experiment on disclosure behavior when shopping online. *Online Information Review*, *45*(3), 537–547. https://doi.org/10.1108/OIR-03-2020-0082

Google. (2017, November). *Consumer barometer study 2017 – The year of the mobile majority*. Author. https://www.thinkwithgoogle.com/intl/en-cee/marketing-strategies/app-and-mobile/consumer-barometer-study-2017-year-mobile-majority/

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate data analaysis*. Prentice Hall.

Hallam, C., & Zanella, G. (2017). Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. *Computers in Human Behavior*, *68*, 217–227. https://doi.org/10.1016/j.chb.2016.11.033

Hawlitschek, F., Notheisena, B., & Teubnerb, T. (2018). The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. *Electronic Commerce Research and Applications*, *29*, 50–63. https://doi.org/10.1016/j.elerap.2018.03.005

Heirman, W., Walrave, M., & Ponnet, K. (2013). Predicting adolescents' disclosure of personal information in exchange for commercial incentives: An application of an extended theory of planned behavior. *Cyberpsychology, Behavior, and Social Networking*, *16*(2), 81–87. https://doi.org/10.1089/cyber.2012.0041

Hofstede, G., Hofstede, G. J., & Minkov, M. (2010). *Cultures and organizations: Software of the mind-intercultural cooperation and its importance for survival*. McGraw Hill.

Lee, H., Lim, D., Kim, H., Zo, H., & Ciganek, A. P. (2015). Compensation paradox: The influence of monetary rewards on user behaviour. *Behaviour & Information Technology*, *34*(1), 45–56. https://doi.org/10.1080/0144929X.2013.805244

Li, H., Sarathy, R., & Xu, H. (2010). Understanding situational online information disclosure as a privacy calculus. *Journal of Computer Information Systems*, *51*(1), 62–71. https://doi.org/10.1080/08874417.2010.11645450

Liang, S., Li, H., Liu, X., & Schuckert, M. (2019). Motivators behind information disclosure: Evidence from Airbnb hosts. *Annals of Tourism Research*, *76*, 305–319. https://doi.org/10.1016/j.annals.2019.03.001

Lu, Y., Ou, C., & Angelopoulos, S. (2018). *Exploring the effect of monetary incentives on user behavior in online sharing platforms* [Conference session]. Proceedings of the 51st Hawaii International Conference on System Sciences, Hawaii, USA (pp. 3437–3444). https://doi.org/10.24251/HICSS.2018.436

Malgieri, G., & Clusters, B. (2018). Pricing privacy – The right to know the value of your personal data. *Computer Law & Security Review*, *34*(2), 289–303. https://doi.org/10.1016/j.clsr.2017.08.006

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336–355. https://doi.org/10.1287/isre.1040.0032

Morey, T., Forbath, T., & Schoop, A. (2015). Customer data: Designing for transparency and trust. *Harvard Business Review*, *93*(5), 96–105.

Mukherjee, S., Manjaly, J. A., & Nargundkar, M. (2013). Money makes you reveal more: Consequences of monetary cues on preferential disclosure of personal information. *Frontiers in Psychology*, *4*, 839. https://doi.org/10.3389/fpsyg.2013.00839

Najjar, M. S., Dahabiyeh, L., & Algharabat, R. S. (2021). Users' affect and satisfaction in a privacy calculus context. *Online Information Review*, *45*(3), 577–598. https://doi.org/10.1108/OIR-02-2019-0054

Pentina, I., Zhang, L., Bata, H., & Chen, Y. (2016). Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison. *Computers in Human Behavior*, *65*, 409–419. https://doi.org/10.1016/j.chb.2016.09.005

Phonthanukitithaworn, C., & Sellitto, C. (2016). A reflection on intercept survey use in Thailand: Some cultural considerations for transnational studies. *The Electronic Journal of Business Research Methods*, *14*(1), 60–70.

Phonthanukitithaworn, C., & Sellitto, C. (2017). Facebook as a second screen: An influence on sport consumer satisfaction and behavioral intention. *Telematics and Informatics*, *34*(8), 1477–1487. https://doi.org/10.1016/j.tele.2017.06.011

Podsakoff, P. M., MacKenzie, S. B., & Podsakoff, N. P. (2012). Sources of method bias in social science research and recommendations on how to control it. *Annual Review of Psychology*, *63*, 539–569. https://doi.org/10.1146/annurev-psych-120710-100452

Prince, C. (2018). Do consumers want to control their persoanl data? Empirical evidence. *International Journal of Human-Computer Studies*, *110*, 21–32. https://doi.org/10.1016/j.ijhcs.2017.10.003

Robinson, C. (2017). Disclosure of personal data in ecommerce: A Cross-national comparison of Estonia and the United States. *Telematics and Informatics*, *34*(2), 569–582. https://doi.org/10.1016/j.tele.2016.09.006

Roth, A. (2017). Pricing information (and its implications). *Communicatoins of the ACM*, *60*(12), 78–79.

Sellitto, C. (2006). Improving winery survey response rates: Lessons from the Australian wine industry. *International Journal of Wine Marketing*, *18*(2), 150–152. https://doi.org/10.1108/09547540610681121

Sellitto, C., & Hawking, P. (2015). Enterprise systems and data analytics: A fantasy football case study. *International Journal of Enterprise Information Systems*, *11*(3), 1–12. https://doi.org/10.4018/IJEIS.2015070101

Shibchurn, J., & Yan, X. B. (2014). *Investigating effects of monetary reward on information disclosure by online social networks users* [Conference session]. Proceedings of the 47th Hawaii International Conference on System Sciences, Waikoloa, HI, USA (pp. 1725–1734). https://doi.org/10.1109/HICSS.2014.220

Statista. (2019, October). *Ownership of wearable tech in Thailand in 2019*. Author. https://www.statista.com/statistics/1051925/thailand-ownership-of-wearable-tech/

Tabachnick, B. G., & Fidell, L. S. (2013). *Using multivariate statistics*. Pearson.

Wang, X., & McClung, S. R. (2010). Toward a detailed understanding of illegal digital downloading intentions: An extended theory of planned behavior approach. *New Media & Society*, *13*(4), 663–677. https://doi.org/10.1177/1461444810378225

Wang, Z., & Liu, Y. (2014). Identifying key factors affecting information disclosure intention in online shopping. *International Journal of Smart Home*, *8*(4), 47–58.

Wu, K. W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior*, *28*(3), 889–897. https://doi.org/10.1016/j.chb.2011.12.008

Wu, P. F. (2019). The privacy paradox in the context of online social networking: A self-identity perspective. *Journal of the Association for Information Science and Technology*, *70*(3), 207–217. https://doi.org/10.1002/asi.24113