Modelling the intended use of Facebook privacy settings.

Abstract:

Background

The ineffective use of Facebook privacy settings has become commonplace. This has made it possible for corporates not only to harvest personal information but also to persuade or influence user behaviour in a manner that does not always protect Facebook users.

Objectives

The objective of this article was to develop a research model that could be used to evaluate the influence of subjective norms, information security awareness and the process of threat appraisal on the intention to use Facebook privacy settings.

Method

In this article, the authors made use of a qualitative approach. Literature pertaining to subjective norms, information security awareness and threat appraisal was thematically analysed using Atlas.ti. Through a process of inductive reasoning, three propositions were developed.

Results

This study found that it is likely that an individual's intention to use Facebook privacy settings will be influenced by subjective norms, information security awareness and the process of threat appraisal. To evaluate the behavioural influence of these selected constructs and relationships, a research model was developed based on both the theory of planned behaviour and protection motivation theory.

Conclusion

In this article, it is argued that the ineffective use of Facebook privacy settings may be because of the behavioural influence of subjective norms. This is compounded by the fact that most users are unaware of privacy threats. This makes these users vulnerable to Facebook-based privacy threats because the process of threat appraisal is conducted with incomplete, inaccurate or missing information.

Full Text:

Author(s): Kimberley Read [1]; Karl van der Schyff (corresponding author) [1]

Introduction

Social interaction via the use of Facebook has become part of over 2 billion users' daily lives (Symeonidis et al. 2018). In some respects, this may be attributed to the fact that users are able to build not only social relationships but also a shared personal identity. Such interaction enables users to engage with Facebook on a psychological level, which in turn satisfies that most users seek, namely recognition and belonging (Debatin et al. 2009). This is exemplified in a recent study, which revealed that, on average, Facebook users check their accounts roughly 14 times a day (Kusyanti et al. 2017). These users also tend to construct their Facebook identities based on the influence of their peers (Strater & Lipford 2008). However, if not protected using Facebook privacy settings, such approaches to self-disclosure often lead to unintended consequences, one being the misuse of personal information. This is especially pertinent given that privacy threats are believed to be a composite result of oversharing personal information paired with the insufficient use of privacy settings. Subjective forces, such as the need to accumulate more Facebook friends, imply that in practice many platform users befriend others who are in actual fact absolute strangers (Govani & Pashley 2014).

As a result, these so-called Facebook friends have access to a number of pieces of personal information. This includes not only those aspects that remain relatively static (i.e. a user's age and gender) but also their thoughts and ideas in the form of Facebook posts and likes. Together, these aspects of a user's profile not only make it possible to enhance Facebook's ability to sell advertising space, but also enable Facebook to monitor and, to some extent, predict a user's online behaviour.

Although targeted advertising has the potential to increase the revenues of social media companies, it is the prediction of user behaviour that allows Facebook to misuse user data. In fact, the ability to monitor content with the intent to manipulate user behaviour is profound (Amer & Noujaim 2019). One only has to consider the numerous voter-profiling campaigns carried out by Cambridge Analytica to appreciate the significance of influencing behaviour by way of posting tailored content to users classified as *persuadable* (Amer & Noujaim 2019). Such classification can only be carried out by harvesting as much personal information as is needed to determine a user's preferences, and possibly even their dominant personality traits. Given that companies like Cambridge Analytica have been able to harvest enough personal information to influence these co-called *persuadables*, it makes sense to understand the behavioural aspects that influence Facebook users' intentions to enact protective behaviour.

Within the context of this article, such protective behaviour is understood as a Facebook user's intention to use privacy settings effectively. It is believed that the use of these settings would limit the inadvertent disclosure and misuse of personal information. To model this influence, the authors of this article have adapted the *theory of planned behaviour* (TPB) by replacing *perceived behavioural control* (PBC) with *information security awareness*, and also incorporated an element of *protection motivation theory* (PMT), namely *threat appraisal*. These constructs are conceptualised as follows: the authors argue that an individual's threat appraisal will influence their intention to use the privacy settings. If an individual is aware of privacy threats, they will likely be more inclined to use the privacy settings. Conversely, if they are not aware of privacy threats, they will be more likely to avoid using privacy settings. *Information security awareness* is conceptualised as the knowledge an individual possesses regarding privacy threats. It is therefore argued that information security awareness controls the effectiveness of an individual's threat appraisal. If they possess little or no knowledge of privacy threats, the process of threat appraisal will be ineffective.

The authors also argue in favour of the behavioural influence of subjective norms. In this context, *subjective norms* are conceptualised as an individual's susceptibility to the views of their peers with respect to the use of privacy settings. If an individual is influenceable, their peers' privacy behaviour will likely influence theirs. In other words, if their peers avoid using privacy settings, so will they.

Together, the behavioural implications of the model described above enable this study to contribute to known theory because few Facebook privacy studies have merged PMT and the TPB in this manner. Although Stern and Salb (2015) evaluated the influence of norms, they did so by incorporating both descriptive and subjective norms, modelling their influence on the intended use of Facebook instead of focusing on privacy settings.

Facebook privacy settings in perspective

Facebook allows users to control their personal information (and profile) through an elaborate system of settings, commonly referred to as Facebook privacy settings. These settings allow users to control the extent to which their peers, and even strangers, can access their personal information (Lewis, Kaufman & Christakis 2008). Users can also see the activities of other users and friends--especially if the content is marked as public (Zlatolas et al. 2015). Some personal information is also made public by default. This includes a user's name, gender, profile picture, cover photo, language, country and age. These pieces of personal information are made available to individuals who may not even have a Facebook profile (Facebook 2019), hence the ease with which companies like Cambridge Analytica can find personal information to misuse or to persuade individuals. To make matters worse, many users are unaware that the default privacy settings allow this type of access.

Nevertheless, users still disclose personal information, making this a relevant and persistent problem. Several explanations have been put forward as possible reasons why the privacy settings are not being used. Some researchers argue in favour of social conformance, implicit trust, poor interface design and permissive default settings (Strater & Lipford 2008). Given the use of *threat appraisal*, this article investigates an individual's perception of threats, specifically threats that pertain to the safety of individuals' social media based personal information. To this extent, a study by Govani and Pashley (2014) found that whilst students were aware of threats (i.e. identity theft, stalking and general misuse), they were still inclined to provide the information and failed to implement protective measures. Research points to three possible reasons why the Facebook privacy settings are not adequately used:

* Users are unaware of any threats.

* Users are apathetically aware of privacy threats.

* Facebook privacy settings are too difficult to use and are therefore avoided.

Dickinson and Holmes (2008) found that individuals are likely to become more evasive and adopt maladaptive coping

responses if the threat level is high, as opposed to proactively reducing the effect of the threat (Marett, Vedadi & Durcikova 2019). Often, fear motivates action in these cases, which may take the form of self-protective or avoidant responses (Witte & Allen 2000).

Whilst privacy options and settings have become more sophisticated (Haynes, Bawden & Robinson 2016), research has found these tools to be underutilised (Boyd & Hargittai 2010; Golbeck & Mauriello 2016). Therefore, the technological aspects of security cannot solely guarantee a secure environment for personal information. Researchers also have to take human aspects into consideration (Safa & Von Solms 2016). Overall, studies have found that users find the Facebook privacy settings confusing, time-consuming and challenging to use. This may in turn result in the accidental or unintentional disclosure of personal information regardless of the additional forms of control users have.

Methodology

This article adopted a qualitative approach as the authors performed in-depth thematic analysis of secondary data.

Data collection

The purpose of this article was to collect data on the behavioural influence of *subjective norms, information security awareness* and *threat appraisal*. This entailed collecting and thematically analysing secondary data obtained from a variety of academic databases as part of a scoping review. These databases included ScienceDirect, Taylor & Francis, Oxford Academic and the AIS Senior Scholars Basket, which include journals like the *European Journal of Information Systems, Information Systems Journal, Information Systems Research* and *MIS Quarterly*. A scoping review is generally used to identify and map available evidence as it relates to a topic of interest (Munn et al. 2018). This required a series of structured searches using phrases such as *information security awareness, threat appraisal, subjective norms, Facebook privacy settings* and *social media*. After screening the titles and abstracts, 42 articles were thematically analysed, as illustrated in the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) diagram shown in Figure 1.

FIGURE 1: Preferred Reporting Items for Systematic Reviews and Meta-Analyses diagram illustrating the search process. [see PDF for image]

Method of analysis

As part of the analysis process, a series of thematic maps were created, one for each of the propositions. This process also involved a more focused review and rereading of the 42 articles - a common practice when conducting thematic analysis (Bowen 2009). Such rereading not only illuminates prominent themes that were not apparent during the initial screening process (Joffe 2012) but also enables researchers to recognise specific patterns. In turn, these patterns may become categories to guide analysis within identified themes. For example, it is reasonable to assume that most (if not all) of the selected studies employed specific research methods. These methods of analysis may become one such analysis category. This entire process was conducted inductively so as to emphasise the researcher's understanding of the broader phenomena pertaining to the use of Facebook privacy settings (Braun & Clarke 2006). A deductive approach was deemed inappropriate for this study, given that the objective of the article was to develop the research model and not to test it using statistical means. As part of the inductive analysis a five-phased approach was used, as outlined by Braun and Clarke (2006). These phases are described as follows:

* becoming acquainted with the data by reading and rereading the selected articles

* developing initial codes (short phrases) in Atlas.ti to describe one or more textual extracts from the selected articles (see Table 1)

* collating codes into potential (or candidate) themes (code groups in Atlas.ti)

* reviewing themes in relation to coded extracts, as well as merging themes if required

* defining and naming these themes, culminating in the development of thematic maps (networks in Atlas.ti).

TABLE 1: Example of coded extracts, associated themes and sources.

Data extract	Atlas.ti codes	Candidate theme	Source
'_ willingly reveal highly personal information if their friends do.'	* ++influence of norms: descriptive	Normative influence	Acquisti and Gross (2006)

Data extract	Atlas.ti codes	Candidate theme	Source
'_ Siponen (2000) suggested that information security policies should take into account the notion of morality and that they should appear to be moral to the employees.'	* ++influence of norms * infosec compliance	Normative influence	Ahluwalia and Merhi (2018)
'ISA can lead to improved IS behaviour and ISP compliance.'	* ++influence of awareness	Information security awareness	Bauer, Bernroider and Chudzikowski (2017)

ISA, Information security awareness; IS, Information security; ISP, Information security policy.

As part of phase 1, the articles were read in detail to develop an overall understanding of the core aspects (influence of subjective norms and information security awareness) of this study. In phase 2, interesting codes were identified based on the nature and the additional behavioural understanding gained after executing phase 1.

Following this, several codes were collated into candidate themes. Phase 3 culminated in the development of three candidate themes, namely threat appraisal, normative influence and the influence of information security awareness. Using these candidate themes as a starting point, phase 4 further refined these themes by removing extraneous coded extracts. This culminated in the formal specification of three thematic maps (see Figure 2 for one example). It is from these thematic maps that the resultant propositions were developed (i.e. as part of phase 5).

FIGURE 2: Partial thematic map used to argue the behavioural influence of subjective norms. [see PDF for image]

Development of propositions

This section first provides an outline of how the TPB (amongst others) and PMT have been used in related studies, followed by a discussion that outlines the development of the propositions for this study.

Theoretical framework

This study utilised both the TPB and PMT. Ajzen (1985), who developed the TPB, conceptualised the strength of intention as an immediate antecedent of behaviour (Kautonen, Van Gelderen & Fink 2015). Thus, the TPB is based on the assumption that most human behaviour takes place as a result of intent, as influenced by personal attitudes, subjective norms and PBC (Grimes & Marquardson 2019; Ham, Jeger & Ivkovic 2015).

Within the context of this study, attitude is defined as the extent to which an individual either positively or negatively value the use of Facebook privacy settings. *Subjective norms* is defined as the social pressure that influences whether an individual will make use of the Facebook privacy settings. *Information security awareness* is defined as the extent to which an individual is aware of the privacy threats that their personal information is exposed to. Protection motivation theory, on the other hand, proposes that behavioural intentions are motivated by the processes of both threat and coping appraisal (Rogers 1975). Note that this study only argues in favour of the behavioural influence of threat appraisal. In this context, threat appraisal necessitates judging the severity of and the vulnerability attached to not making use of Facebook privacy settings. For example, if a Facebook user determines that their level of self-efficacy is particularly high, they may forgo the privacy settings because they believe they are adequately equipped to ameliorate future threats (i.e. misuse of personal information). Additionally, PMT has been found to adequately explain individuals' behavioural intention to engage in protective actions (Ifinedo 2012).

The research model for this study merges these two theories by arguing the influence of *threat appraisal*, specifically in terms of the role played by fear appeals in the appraisal process. In other words, the research model posits that it is likely that an individual will increase their knowledge of (in terms of avoidance) specific threats as they become aware of vulnerabilities. For example, a Facebook user may wish to find out how they can avoid inadvertently sharing personal information because they fear that it may be misused.

This combination of theoretical constructs not only contributes theoretically but also enables researchers to evaluate the role of fear appeals (one part of threat appraisal) within the context of Facebook privacy settings. The integration of subjective norms further increases the explanatory power of the research model (Tsai et al. 2016). Having said this, other studies have also combined these two theories (Grimes & Marquardson 2019; Ifinedo 2012).

The process by which individuals *weigh up* the costs and benefits of using privacy settings can also be explained by *deterrence theory* (DT) or simply cost-benefit analysis, both of which involve a cognitive process of weighing up the potential

costs and benefits of enacting specific behaviour (Min & Kim 2015). More specifically, DT is based on the belief that sanctions affect an individual's intention to participate in deviant behaviour, depending on the sanction severity, celerity and certainty of the particular behaviour (Abed & Weistroffer 2016). As such, individual behaviour is assumed to be driven by some punishment associated with not performing the required behaviour. Because the use of Facebook privacy settings cannot be enforced, theories that imply forms of sanction (such as DT) are not deemed relevant in this context.

The behavioural influence of subjective norms

Research provides evidence of two distinct sub-types of social norms, namely subjective and descriptive norms (Lapinski & Rimal 2005). Descriptive norms are those perceptions of the behaviour that an individual's peers are enacting. As such, they describe a behaviour that has taken or is taking place. Conversely, subjective norms are those behaviours believed to be desired by an individual's peers (Kautonen et al. 2015). Subjective norms therefore assume that individuals are more likely to enact a behaviour that they believe is desired or expected by their peers (Saeri et al. 2014).

Both descriptive and subjective norms are believed to drive an individual's behaviour towards social acceptance (Min & Kim 2015). Such acceptance even takes place to the extent that individuals may adjust their norms if they differ from the normative required behaviour. These adjustments may reinforce or counter the normative behaviour depending on how closely individuals identify with their peers (White et al. 2009). If, for example, an individual's peers do not place much emphasis on sustainability, they may avoid associated behaviours.

It should be noted that although subjective norms influence behaviour, they depend on the user population (and use case) in question. For example, subjective norms have been found to significantly influence game use but not the use of blogs (Baek, Kim & Bae 2014). Because the use of games and blogs includes voluntary settings, Baek et al.'s argument relates to how strongly individuals perceive general behavioural rules to exist within these contexts. Individuals might perceive sanctions to exist if normative behaviour is not followed in gaming, which is not the case when using blogs.

From a social media perspective, subjective norms have been found to affect the problematic use of Facebook, specifically amongst adolescents (Marino et al. 2016). Some research suggests that this is the result of adolescents being more concerned about having their personal information accessed by people who hold immediate power over them (i.e. parents or teachers) (Boyd & Hargittai 2010). To substantiate the latter, Foltz Newkirk and Schwager (2016) found that although subjective norms positively influenced Master of Business Administration (MBA) students' intention to use social media privacy settings, they exerted a relatively weak influence on intent.

Previous research has reported mixed outcomes regarding the behavioural influence of subjective norms; specifically, whether it negatively or positively influences intent. Whilst some research has found subjective norms to be the weakest predictor of intention (Ham et al. 2015; Min & Kim 2015), other studies have concluded that they have a significant influence on intention (Grimes & Marquardson 2019) and that they shape not only behavioural intentions but also the subsequent behaviour of an individual (Chung & Rimal 2016). This discrepancy in the literature may depend on the type of behaviour under consideration, the individual involved or how closely the individual identifies with significant others (White et al. 2009). It may also depend on perceptions regarding the perceived costs of non-conformance (Min & Kim 2015). Previous studies also suggest that norms are only meaningful to the extent that individuals perceive that their violation will result in some punishment or repercussion (e.g. the misuse of their personal information) (Chalub, Santos & Pacheco 2006). Given the discussion thus far, the following proposition is made:

Proposition 1 (P1): Subjective norms will influence an individual's intention to use Facebook privacy settings.

The influence of information security awareness

The literature is replete with evidence that information security awareness influences behaviour as a form of control (hence substituting it for PBC in this article). The more aware and knowledgeable a user becomes with regard to possible privacy threats, the more control they might wish to have in this regard, one such control mechanism being the Facebook privacy settings. The authors therefore argue that individuals can only take adequate protective measures once they have been made aware of the threats associated with exercising no control over their personal information (Öütçü, Testik & Chouseinoglou 2016). If users are not aware of the tools to protect them against threats (i.e. misuse of personal information), they will not acquire the requisite knowledge to adopt effective protective measures. Instead, these users may be unaware that Facebook provides them with tools such as the *Privacy Checkup* tool. This may lead to protective behaviours being enacted under false assumptions of security (Golbeck & Mauriello 2016), which may increase overall vulnerability. This affects not only these individuals but also their peers (i.e. the bidirectional relationship indicated by the dotted lines in Figure 3). Conversely, it stands to reason that if a Facebook user acts on the information received from peers (therefore increasing awareness), they may develop intentions to use the privacy settings. In doing so, this individual also inadvertently influences their peers to enact the same protective behaviour.

FIGURE 3: Proposed research model. [see PDF for image]

Although the bidirectional relationship between an individual's attitude towards privacy and awareness is not argued in this

article, it plays a vital role when viewing the use of privacy settings holistically. In other words, the behavioural influence of the various theoretical constructs proposed by this study does not affect the intended use in a mutually exclusive manner. In general, awareness has been found to contribute to the behaviour of individuals in several contexts. Park, Kim and Park (2017) found that awareness of patient privacy amongst nursing students has a significant impact on behaviours to enact protective behaviour when considering the security of patients' personal information. Within the context of this article, awareness is assumed to have the same effect on the use of privacy settings.

Therefore, information security awareness measures the extent to which users are informed about their privacy on social networking sites, as well as the extant privacy problems, policies, violations and procedures (Zlatolas et al. 2015). Uninformed users fail to evaluate the privacy risk and information disclosure benefits rationally and thoroughly. As a result, lack of awareness is viewed as a root cause of information security incidents (Safa et al. 2018). Grimes and Marquardson (2019) found that if a user does not perceive any threats arising as a result of a particular action or behaviour, no protective measures will be taken. Therefore, in order to promote more secure online behaviour, as mentioned, users first need to be made aware of both the threats associated with the disclosure of personal information and the tools available to protect against those threats (e.g. privacy settings).

In industry, awareness programmes have been implemented to improve users' compliance and promote secure user behaviour. Bauer et al. (2017) indicate that a user's level of policy knowledge affects their intentions to comply with such policies. Businesses like Facebook have also begun relying on privacy policies as a self-regulatory mechanism in an attempt to reassure users that their personal information is secure (Benson, Saridakis & Tennakoon 2015).

Conversely, in a study by Govani and Pashley (2014), it was found that even though 84% of participants were aware that they could change their privacy settings, only 48% actually used these settings. Additionally, respondents did not change their privacy settings even after being educated on how to do so. Users therefore seemingly accept that their personal information will be misused, regardless of whether they enact protective behaviour (i.e. Facebook privacy settings). Respondents' awareness and the consequent privacy concerns only resulted in the adoption of protective behaviour if they have had a negative experience in this regard. As such, knowledge, awareness and especially experience are seen to directly influence the intention to adopt protective behaviour such as Facebook privacy settings. The authors of this article therefore argue that:

Proposition 2 (P2): Information security awareness will influence an individual's intention to use Facebook privacy settings.

The behavioural influence of threat appraisal

The authors also argue that that the adoption of protective behaviour goes beyond merely making users aware. They posit that the acquired knowledge (via awareness) has to be personally relevant if individuals are to respond appropriately (Marett et al. 2019). Additionally, the individual should be willing and able to respond effectively.

Because PMT is concerned with how and why individuals decide to adopt protective behaviour (e.g. adopting privacy settings), the authors argue that it will also influence the extent to which such protective behaviour is enacted. This stems from the fact that an individual's threat appraisal involves the measurement of the perceived vulnerability and the severity of the threat. Therefore, if an individual does not perceive a threat to be particularly severe (because of their level of knowledge and awareness), they may forgo using privacy settings. Previous research has found user perceptions to be particularly important when facing decisions relating to protective behaviour - especially within the context of fear appeals (Johnston et al. 2016). It is believed that should threat appraisal produce a sufficient amount of fear, the individual will be more likely to enact protective behaviour. This means that their level of fear - as a result of threat appraisal - may influence their intention to use privacy settings.

Similar to Hanus and Wu (2016), this study focuses on both awareness and threat appraisal as antecedents to the intended use of Facebook privacy settings. Hanus and Wu's (2016) study also demonstrates that it is not enough for users to be aware of the threats associated with a particular behaviour. Users are also influenced by their perceptions of how vulnerable they may be in this regard. The same applies to the countermeasures used to address the perceived threats. As such, awareness alone does not help promote secure behaviour, which is why the model proposed in this article also theorises the behavioural influence of threat appraisal.

Several recent studies have found evidence that attests to the behavioural influence of threat appraisal. For example, Strycharz et al. (2019) found that threat appraisal (specifically perceived severity) significantly influenced respondents' intentions to turn off personalisation in terms of the ads they are exposed to. Similarly, Feng and Xie (2019) found that respondents' control over privacy settings significantly influenced their intention to use virtual try-on (i.e. of clothing) apps. The additional controls enabled respondents to perceive themselves to be less vulnerable to threats. Vishwanath, Xu and Ngoh (2018) found that perceived threat severity significantly influences both expressive privacy and information privacy. Additionally, perceived vulnerability was found to influence accessibility privacy. Ernst, Pfeiffer and Rothlauf (2015) also found threat appraisal to exert a significant and positive influence on the intention to use the privacy settings, specifically in terms of selectivity in connections, refusal and setting strictness. Whilst a heightened threat appraisal is associated with fear (Grimes & Marquardson 2019), a user can only evaluate a risky situation if they are aware of the risks. The authors of this

article therefore propose:

Proposition 3 (P3): The process of threat appraisal will influence a Facebook user's intention to use privacy settings.

Ethical consideration

This article followed all ethical standards for a research without direct contact with human or animal subjects.

Discussion

The proposed research model is an adapted version of both the TPB and PMT (see Figure 3). In this model, the construct PBC is replaced by *information security awareness*. Both *subjective norms* and *threat appraisal* are modelled as having a direct influence on the construct *intention to use privacy settings*. Note that the authors do not directly argue the behavioural influence of the dotted lines in the proposed research model. This also applies to the sub-components of the construct *threat appraisal* (i.e. vulnerability and severity) and demographic aspects, including negative privacy experiences. The influence of information security awareness on the actual use of privacy settings is also outside the scope of this article.

The use of this research model allows researchers to understand how both threat appraisal (P3) and information security awareness (P2) influence the use of Facebook privacy settings. The model also allows for the evaluation of the influence exerted by subjective norms (P1). The authors argue that awareness alone is not enough to understand individuals' intentions to enact protective behaviour. Instead, the authors posit that even though individuals are aware of information misuse, they may still avoid the use of privacy settings because they do not perceive the threat to be severe. Therefore, the personal information they disclose is not perceived as sufficiently important to misuse, and even if it is misused, not much harm can be done. The authors argue that this is not necessarily the case, especially if one considers that the influence exerted may have far-reaching implications beyond just the use of Facebook and personal information. Consider the use of cleverly designed posts that appear only to individuals deemed susceptible. Here, even just sharing one's gender can be used to display messages that may invoke sympathy or higher than usual levels of fear. Abnormal levels of fear, resulting from raised levels of awareness, could be used to manipulate users. Recent evidence in the form of voter profiling is but one example. Additionally, it is known that women are more sympathetic and generally more concerned about what their peers think of their behaviour and are thus influenceable (Tifferet 2019). By using the proposed research model, researchers will be able to get some indication of the extent to which subjective norms influence not only these individuals but also their peers. In doing so, the message is perpetuated, resulting in successful persuasion of an individual deemed persuadable, as alluded to in the 'Introduction' section.

Because the proposed model does not focus on other individual differences and specific psychological aspects, it is useful in instances where even a minimal amount of information is not adequately protected by the privacy settings. This makes it particularly useful in providing researchers with an initial description as to what to focus on going forward. Further statistical evaluation of this model may indicate that fear appeals, as evoked during the process of threat appraisal, do not exert a significant influence on the intended use of privacy settings.

The thematic analysis further suggests that subjective norms will exert a significant influence on the intention to use privacy settings. Given the social nature of Facebook, this is not only expected but is also important to model - especially in relation to demographic aspects. The results could be used to make Facebook users aware of the extent that even minimal amounts of personal information could be used to manipulate their behaviour, which inadvertently also influences their peers. Results may indicate that this is more pronounced for women. Thus, models like the one the authors propose here could be useful to social media platforms in that it is their responsibility to educate and make users aware of their level of susceptibility. This is exactly what Mark Zuckerberg (chief executive officer of Facebook) alluded to in his senate hearing (Timberg, Romm & Dwoskin 2018), where he essentially stated that the company did not do enough to prevent the misuse of its users' personal information. The use of similar models may thus assist in this regard.

Limitations

Because this study developed a research model from thematic interpretations, the resultant arguments are influenced by the authors' ideological frame of reference. It stands to reason that future work may develop similar models using different arguments. Additionally, although this study conducted a scoping review, as opposed to a more rigid structured review, only a limited number of secondary sources formed part of the thematic analysis. Moreover, arguments supporting the other theoretical relationships (indicated by the dotted lines in Figure 3) were omitted because of space limitations. Lastly, no statistical measures were developed and aligned with the constructs of the research model in this article.

Conclusion and future research

In this article, the authors used a thematic approach to inductively analyse a set of secondary data sources. This in turn resulted in the identification of three themes and associated thematic maps (see Figure 2). Using these thematic maps, three corresponding propositions were developed and integrated into an adapted research model consisting of components of both the TPB and PMT. To deductively evaluate the adapted research model, future research could conduct appropriate statistical analyses. For example, a covariance approach to structural equation modelling (CB-SEM) could be used to

evaluate the predictive power (R^2) of the resultant structural model. The use of a CB-SEM approach is particularly important, because the proposed model is recursive in nature, as opposed to a non-recursive version (i.e. without the bidirectional relationships), which could also be evaluated using a partial least squares path modelling.

Acknowledgements

Competing interests

Authors' contributions

Funding information

Data availability statement

Data sharing is not applicable to this article as no new data were created or analysed in this study.

Disclaimer

The views and opinions expressed in this article are those of the authors and do not necessarily reflect the official policy or position of any affiliated agency of the authors.

References

Abed, J. & Weistroffer, H.R., 2016, 'Understanding deterrence theory in security compliance behavior: A quantitative meta-analysis approach', in Proceedings of the Southern Association for Information Systems Conference, SAIS, pp. 1-7, St. Augustine, FL.

Acquisti, A. & Gross, R., 2006, 'Imagined communities: Awareness, information sharing, and privacy on the Facebook', *Privacy Enhancing Technologies* 4258, 36-58. https://doi-org.rlib.pace.edu/10.1007/11957454_3

Ahluwalia, P. & Merhi, M.I., 2018, 'Moral and subjective norms: How do they effect information security compliance?', in Proceedings of the 24th Americas Conference on Information Systems, AMCIS, pp. 1-10, New Orleans, LA.

Ajzen, I., 1985, 'From intentions to actions: A theory of planned behavior', in J. Kuhl & J. Beckmann (eds.) *Action control: From cognition to behavior*, pp. 11-39, Springer, Berlin.

Amer, K. & Noujaim, J., 2019, 'The great hack', *Netflix*, viewed n.d., from https://www.netflix.com/za/title/80117542.

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', *Computers in Human Behavior* 31, 2414-2419. https://doi-org.rlib.pace.edu/10.1016/j.chb.2013.10.010

Bauer, S., Bernroider, E.W.N. & Chudzikowski, K., 2017, 'Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks', *Computers & Security* 68, 145-159. https://doi-org.rlib.pace.edu/10.1016/j.cose.2017.04.009

Benson, V., Saridakis, G. & Tennakoon, H., 2015, 'Information disclosure of social media users: Does control over personal information, user awareness and security notices matter?', *Information Technology and People* 28(3), 426-441. https://doi-org.rlib.pace.edu/10.1108/ITP-10-2014-0232

Bowen, G.A., 2009, 'Document analysis as a qualitative research method', *Qualitative Research Journal* 9(2), 27-40. https://doi-org.rlib.pace.edu/10.3316/QRJ0902027

Boyd, D. & Hargittai, E., 2010, 'Facebook privacy settings: Who cares?', *First Monday: Peer-Reviewed Journal on the Internet* 15(8). https://doi-org.rlib.pace.edu/10.5210/fm.v15i8.3086

Braun, V. & Clarke, V., 2006, 'Using thematic analysis in psychology', *Qualitative Research in Psychology* 3(2), 77-101. https://doi-org.rlib.pace.edu/10.1191/1478088706qp063oa

Chalub, F.A.C.C., Santos, F.C. & Pacheco, J.M., 2006, 'The evolution of norms', *Journal of Theoretical Biology* 241(2), 233-240. https://doi-org.rlib.pace.edu/10.1016/j.jtbi.2005.11.028

Chung, A. & Rimal, R.N., 2016, 'Social norms: A review', *Review of Communication Research* 4, 1-28.

Debatin, B., Lovejoy, J.P., Horn, A.-K. & Hughes, B.N., 2009, 'Facebook and online privacy: Attitudes, behaviors, and unintended consequences', *Journal of Computer-Mediated Communication* 15(1), 83-108. https://doi-org.rlib.pace.edu /10.1111/j.1083-6101.2009.01494.x

Dickinson, S.J. & Holmes, M., 2008, 'Understanding the emotional and coping responses of adolescent individuals exposed to threat appeals', *International Journal of Advertising* 27(2), 251-278. https://doi-org.rlib.pace.edu/10.1080 /02650487.2008.11073054

Ernst, H., Pfeiffer, J. & Rothlauf, F., 2015, 'Privacy protecting behavior in social network sites', in C-P.H. Ernst (ed.), *Factors driving social network site usage*, pp. 1-9, Springer, Wiesbaden.

Facebook, 2019, *What is public information on Facebook?*, viewed 01 April 2020, from https://www.facebook.com /help/203805466323736

Feng, Y. & Xie, Q., 2019, 'Privacy concerns, perceived intrusiveness, and privacy controls: An analysis of virtual try-on apps', *Journal of Interactive Advertising* 19(1), 43-57. https://doi-org.rlib.pace.edu/10.1080/15252019.2018.1521317

Foltz, B.B., Newkirk, H.E. & Schwager, P.H., 2016, 'An empirical investigation of factors that influence individual behavior toward changing social networking security settings', *Journal of Theoretical and Applied Electronic Commerce Research* 11(2), 1-15. https://doi-org.rlib.pace.edu/10.4067/S0718-18762016000200002

Golbeck, J. & Mauriello, M., 2016, 'User perception of Facebook app data access: A comparison of methods and privacy concerns', *Future Internet* 8(2), 9. https://doi-org.rlib.pace.edu/10.3390/fi8020009

Govani, T. & Pashley, H., 2014, 'Student awareness of the privacy implications when using Facebook', *Cyberpsychology* 8(2), 1-17.

Grimes, M. & Marquardson, J., 2019, 'Quality matters: Evoking subjective norms and coping appraisals by system design to increase security intentions', *Decision Support Systems* 119, 23-34. https://doi-org.rlib.pace.edu/10.1016/j.dss.2019.02.010

Ham, M., Jeger, M. & Ivkovic, A.F., 2015, 'The role of subjective norms in forming the intention to purchase green food', *Economic Research-Ekonomska Istrazivanja* 28(1), 738-748. https://doi-org.rlib.pace.edu/10.1080/1331677X.2015.1083875

Hanus, B. & Wu, Y., 2016, 'Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective', *Information Systems Management* 33(1), 2-16. https://doi-org.rlib.pace.edu/10.1080/10580530.2015.1117842

Haynes, D., Bawden, D. & Robinson, L., 2016, 'A regulatory model for personal data on social networking services in the UK', *International Journal of Information Management* 36(6), 872-882. https://doi-org.rlib.pace.edu/10.1016 /j.ijinfomgt.2016.05.012

Ifinedo, P., 2012, 'Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory', *Computers & Security* 31(1), 83-95. https://doi-org.rlib.pace.edu/10.1016 /j.cose.2011.10.007

Joffe, H., 2012, *Qualitative research methods in mental health and psychotherapy: A guide for students and practitioners*, pp. 209-223, Wiley-Blackwell, New York, NY.

Johnston, A.C., Warkentin, M., McBride, M. & Carter, L., 2016, 'Dispositional and situational factors: Influences on information security policy violations', *European Journal of Information Systems* 25(3), 231-251. https://doi-org.rlib.pace.edu /10.1057/ejis.2015.15

Kautonen, T., Van Gelderen, M. & Fink, M., 2015, 'Robustness of the theory of planned behavior in predicting entrepreneurial intentions and actions', *Entrepreneurship Theory and Practice* 39(3), 655-674. https://doi-org.rlib.pace.edu/10.1111 /etap.12056

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 Computer Science* 124, 632-638. https://doi-org.rlib.pace.edu/10.1016/j.procs.2017.12.199

Lapinski, M.K. & Rimal, R.N., 2005, 'An explication of social norms', *Communication Theory* 15(2), 127-147. https://doi-org.rlib.pace.edu/10.1111/j.1468-2885.2005.tb00329.x

Lewis, K., Kaufman, J. & Christakis, N., 2008, 'The taste for privacy: An analysis of college student privacy settings in an online social network', *Journal of Computer-Mediated Communication* 14(1), 79-100. https://doi-org.rlib.pace.edu/10.1111 /j.1083-6101.2008.01432.x

Marett, K., Vedadi, A. & Durcikova, A., 2019, 'A quantitative textual analysis of three types of threat communication and subsequent maladaptive responses', *Computers & Security* 80, 25-35. https://doi-org.rlib.pace.edu/10.1016/j.cose.2018.09.004

Marino, C., Vieno, A., Pastore, M., Albery, I.P., Frings, D. & Spada, M.M., 2016, 'Modeling the contribution of personality, social identity and social norms to problematic Facebook use in adolescents', *Addictive Behaviors* 63, 51-56. https://doi-org.rlib.pace.edu/10.1016/j.addbeh.2016.07.001

Min, J. & Kim, B., 2015, 'How are people enticed to disclose personal information despite privacy concerns in social network sites? The calculus between benefit and cost', *Journal of the Association for Information Science and Technology* 66(4), 839-857. https://doi-org.rlib.pace.edu/10.1002/asi.23206

Munn, Z., Peters, M.D.J., Stern, C., Tufanaru, C., McArthur, A. & Aromataris, E., 2018, 'Systematic review or scoping review? Guidance for authors when choosing between a systematic or scoping review approach', *BMC Medical Research Methodology* 18(143), 1-7. https://doi-org.rlib.pace.edu/10.1186/s12874-018-0611-x

Öütçü, G., Testik, Ö.M. & Chouseinoglou, O., 2016, 'Analysis of personal information security behavior and awareness', *Computers & Security* 56, 83-93. https://doi-org.rlib.pace.edu/10.1016/j.cose.2015.10.002

Park, E.H., Kim, J. & Park, Y.S., 2017, 'The role of information security learning and individual factors in disclosing patients' health information', *Computers & Security* 65, 64-76. https://doi-org.rlib.pace.edu/10.1016/j.cose.2016.10.011

Rogers, R.W., 1975, 'A protection motivation theory of fear appeals and attitude change', *The Journal of Psychology* 91(1), 93-114. https://doi-org.rlib.pace.edu/10.1080/00223980.1975.9915803

Saeri, A.K., Ogilvie, C., La Macchia, S.T., Smith, J.R. & Louis, W.R., 2014, 'Predicting Facebook users online privacy protection: Risk, trust, norm focus theory, and the theory of planned behavior', *Journal of Social Psychology* 154(4), 352-369. https://doi-org.rlib.pace.edu/10.1080/00224545.2014.914881

Safa, N.S. & Von Solms, R., 2016, 'An information security knowledge sharing model in organizations', *Computers in Human Behavior* 57, 442-451. https://doi-org.rlib.pace.edu/10.1016/j.chb.2015.12.037

Safa, N.S., Maple, C., Watson, T. & Von Solms, R., 2018, 'Motivation and opportunity based model to reduce information security insider threats in organisations', *Journal of Information Security and Applications* 40, 247-257. https://doi-org.rlib.pace.edu/10.1016/j.jisa.2017.11.001

Stern, T. & Salb, D., 2015, 'Examining online social network use and its effect on the use of privacy settings and profile disclosure', *Bulletin of Science, Technology & Society* 35(1-2), 25-34. https://doi-org.rlib.pace.edu/10.1177/0270467615596890

Strater, K. & Lipford, H., 2008, 'Strategies and struggles with privacy in an online social networking community', in Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction, BCS-HCI, pp. 111-119, Liverpool.

Strycharz, J., Van Noort, G., Smit, E. & Helberger, N., 2019, 'Protective behavior against personalized ads: Motivation to turn personalization off', *Cyberpsychology* 13(2), 1-22. https://doi-org.rlib.pace.edu/10.5817/CP2019-2-1

Symeonidis, I., Biczók, G., Shirazi, F., Pérez-Solà, C., Schroers, J. & Preneel, B., 2018, 'Collateral damage of Facebook third-party applications: A comprehensive study', *Computers & Security* 77, 179-208. https://doi-org.rlib.pace.edu/10.1016/j.cose.2018.03.015

Tifferet, S., 2019, 'Gender differences in privacy tendencies on social network sites: A meta-analysis', *Computers in Human Behavior* 93, 1-12. https://doi-org.rlib.pace.edu/10.1016/j.chb.2018.11.046

Timberg, C., Romm, T. & Dwoskin, E., 2018, 'Zuckerberg apologizes, promises reform as senators grill him over Facebook's failings', viewed 01 April 2020, from https://www.washingtonpost.com/business/technology/2018/04/10/b72c09e8-3d03-11e8-974f-aacd97698cef_story.html.

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', *Computers & Security* 59, 138-150. https://doi-org.rlib.pace.edu/10.1016/j.cose.2016.02.009

Vishwanath, A., Xu, W. & Ngoh, Z., 2018, 'How people protect their privacy on Facebook: A cost-benefit view', *Journal of the Association for Information Science and Technology* 69(5), 700-709. https://doi-org.rlib.pace.edu/10.1002/asi.23894

White, K.M., Smith, J.R., Terry, D.J., Greenslade, J.H. & Blake, M., 2009, 'Social influence in the theory of planned behaviour

: The role of descriptive, injunctive, and ingroup norms', *Society* 48(1), 135-158. https://doi-org.rlib.pace.edu/10.1348/014466608X295207

Witte, K. & Allen, M., 2000, 'A meta-analysis of fear appeals: Implications for effective public health campaigns', *Health Education & Behavior* 27(5), 591-615. https://doi-org.rlib.pace.edu/10.1177/109019810002700506

Zlatolas, L.N., Welzer, T., HeriCko, M. & Hölbl, M., 2015, 'Privacy antecedents for SNS self-disclosure: The case of Facebook', *Computers in Human Behavior* 45, 158-167. https://doi-org.rlib.pace.edu/10.1016/j.chb.2014.12.012

Author Affiliation(s):

[1] Department of Information Systems, Faculty of Commerce, Rhodes University, Grahamstown, South Africa

Author Note(s):

Corresponding author: Karl van der Schyff, k.vanderschyff@ru.ac.za

Note(s):