



# Social media surveillance: A personality-driven behaviour model

**Authors:**

Karl van der Schyff<sup>1</sup>   
Stephen Flowerday<sup>1</sup> 

**Affiliations:**

<sup>1</sup>Department of Information Systems, Rhodes University, Grahamstown, South Africa

**Corresponding author:**

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

**Dates:**

Received: 12 Sept. 2018  
Accepted: 20 Feb. 2019  
Published: 13 June 2019

**How to cite this article:**

Van der Schyff, K. & Flowerday, S., 2019, 'Social media surveillance: A personality-driven behaviour model', *South African Journal of Information Management* 21(1), a1034. <https://doi.org/10.4102/sajim.v21i1.1034>

**Copyright:**

© 2019. The Authors.  
Licensee: AOSIS. This work is licensed under the Creative Commons Attribution License.

**Read online:**

Scan this QR code with your smart phone or mobile device to read online.

**Background:** The use of third-party Facebook apps have become a common occurrence. However, this leads to problems such as information misuse, because many Facebook apps are able to build accurate behavioural and usage profiles which users are unaware of.

**Objectives:** The aim of this article was to develop a research model that could be used to evaluate the influence of awareness and personality on the intent to use third-party Facebook apps.

**Method:** In this article, we took a qualitative approach to code awareness and personality related literature using Atlas.ti software. After reviewing the codes, propositions were created and integrated into an adapted version of the Theory of Planned Behaviour.

**Results:** The study found that it is likely that individuals' personality type will influence their intent to use third-party Facebook apps. It also found evidence to suggest that awareness of social media surveillance will influence a user's intent to use third-party Facebook apps. Based on the review, the article proposes the use of an adapted version of the Theory of Planned Behaviour by incorporating information security awareness of social media surveillance.

**Conclusion:** Although social media surveillance is commonplace, much of it is conducted for commercial purposes without users being aware thereof. This article concludes that it is possible to determine a Facebook user's susceptibility to social media surveillance via third-party apps by evaluating the combined influence of personality type and awareness.

**Keywords:** Facebook; surveillance; personality types; information security awareness; Theory of Planned Behaviour.

## Introduction

For many Internet users, participating in social networking has become a daily routine (Hallam & Zanella 2017; Li, Lin & Wang 2015). Such participation allows users not only to share content with friends and family (Chen, Sharma & Rao 2016) but also to accumulate social capital whilst developing psychosocial networks (Hallam & Zanella 2017). With more than 2 billion active users (Jafarkarimi et al. 2016), Facebook and social networks in general have become lucrative commercial environments for businesses because of the ability to market to a large captive audience with relative ease (Vladlena et al. 2015). For example, targeted advertising no longer relies on the completion of lengthy and time-consuming consumer surveys. Rather, corporates use location-based services (LBS) to pinpoint the places users frequent. When combined with data related to a social media profile, corporates like Facebook can create rich descriptions of their users' behavioural patterns. Not only are the resultant data assemblages (combination of location and profile data) useful for improving the services delivered by Facebook but also they are useful as a commodity – one that can be sold to third-party organisations as a form of information misuse (Fuchs 2012).

However, third-party organisations do not have to rely only on Facebook to create such data assemblages. Third parties could, for example, also develop apps that users elect to access using their Facebook credentials. This allows for the harvesting of user data through the linked app by utilising application programming interfaces (APIs) (Koban et al. 2018). In this way, third parties are able to combine the usage data of their app with the profile data on Facebook. A controversial example of this is the use of personal information by Cambridge Analytica. By determining the personality types of Facebook users, this organisation was able to gain insight into the possible voting behaviour of these users (Confessore 2018). In this case, a third-party app was developed (thisisyourdigitallife) with the intent to determine a user's personality type; at least this was communicated to the user as such (Symeonidis et al. 2018). However, unbeknownst to the user,

this data set was combined with their Facebook profile (they had to sign in with their Facebook credentials) and the resultant data assemblage was misused. As such, it seems that users are unaware of how their personal information may be used by not only social media sites but also the third-party apps they elect to link to their social media profiles.

Given that the behaviour of a user is influenced by his or her personality (Moore & McElroy 2012) and users are seemingly unaware of how their personal information is used (Wagner et al. 2018), this article sets out to explore how personality types and awareness influence a user's behavioural intent to make use of third-party apps on social media – Facebook in particular. The article contributes by developing a research model that can be used to ascertain how susceptible an individual is to social media surveillance (SMS). To determine this, the model evaluates both the influence of a user's personality type and awareness of SMS on their attitude towards the use of third-party Facebook apps. Because the research model evaluates human behaviour, it is based on the Theory of Planned Behaviour (TPB).

The article is structured as follows: firstly, the reader is presented with a discussion on the extent of Facebook surveillance, followed by a discussion on the methodological approach used in this article. This is followed by a review of related studies detailing the findings of other researchers who have studied behavioural information security by investigating the influence of personality types and awareness. From the preceding discussion, we create two propositions and illustrate them on an adapted version of TPB in the form of a research model.

### Extent of Facebook surveillance

As one of the largest social media websites, Facebook has made extensive commercial use of its users' profile data over a number of years (Lyon 2014; Mamonov & Benbunan-Fich 2018). Such data are not only used to improve its service offerings but also to fund its operations. With a daily user count of 1.52 billion active users (as of December 2018), Facebook has access to large amounts of data related to user behaviour (Chang & Chen 2014). For example, with the widespread adoption of mobile devices, Facebook has made extensive use of LBS to leverage such data sets. Everything users post and do on the platform is commodified and although such interactions enrich the Facebook experience, they raise a myriad of information privacy concerns (Chang & Chen 2014).

These concerns include privacy settings that are a challenge to use, the creation of algorithm-driven data assemblages by third-party apps, users not taking adequate responsibility for their personal information and a general lack of awareness of the aforementioned issues (Jeong & Kim 2017; Jordaan & Van Heerden 2017; Lee, Hansen & Lee 2016; Symeonidis et al. 2018; Taneja, Vitrano & Gengo 2014). For example, Symeonidis et al. (2018) found that such inadequate privacy settings, as well as suboptimum server communications made

it easy to retrieve personal information via a third-party app. Using the AppInspect data set, Symeonidis et al. (2018) demonstrated that app developers can not only extract data from one app but also combine the data of a single Facebook user across several apps – mainly because most app developers usually own and operate more than one app. A case in point is Telaxo, which operates 118 apps, with more than 10000 users actively using these apps. Over and above directly accessing the personal information of Facebook users, these app providers are able to gain indirect access to the Facebook users' friends. One example is TripAdvisor, which collects information on the user's location, residence and 'likes'. This information is then inadvertently also available to the user's friends to keep track of locations they may have both visited in the past. Collating such information allows TripAdvisor to better understand not only travel behaviour but also the common personal traits of the individuals who visited a specific location of interest. Even Facebook-based games are used in this manner. For instance, Symeonidis et al. (2018) found that if a user installs Candy Crush Saga, the app not only collects the user's profile name but also his or her profile picture and country of residence. Like TripAdvisor, the app collects the user's entire friend list. Most importantly, the users are unaware of this.

Facebook users' lack of responsibility could also be exploited when viewing social media sites as environments where users only engage in a personal capacity. Rather, users rarely assume responsibility, to the extent that the privacy consequences are assessed at an organisational level, which is where information is often misused by third parties (Barth & De Jong 2017). This is confirmed by Chang and Chen (2014), who found that users of both Sociallight and Foursquare (both LBS platforms) were more interested in the ability to strengthen social relations than assessing the information privacy concerns at an organisational level. Similar results are reported by Tariq et al. (2017), who found that many Facebook users voluntarily adjust their privacy settings to keep track of their friends' whereabouts, as well as to stay open to additional contacts. Further (and more recent) evidence is provided in the form of the sheer magnitude (300 million, circa 2017) of personal photos that are shared by Facebook users on a daily basis (Mamonov & Benbunan-Fich 2018). This happens despite the number of information security breaches that have occurred since January 2017 (i.e. Adidas, Macy's, Kmart, Delta Airlines and Under Armour), which in some instances resulted in the loss of users' personal information (Green & Hanbury 2018). Thus, the collection and distribution of personal information on social media sites (via third-party apps) exceed what users assume, expect and are aware of.

### Research methods and design

To select relevant literature, we used a systematic approach. Specific search phrases were selected to conduct initial searches on several academic databases. Phrases such as *theory of planned behavior/behaviour*, *awareness*, *personality type/trait* and *individual differences* were used in various combinations on a number of academic databases, which included the likes of

ScienceDirect, Sabinet, Scopus, ACM, AISLnet, Google Scholar (via Publish or Perish) and the IS Senior Scholars Basket of Journals. All the searches were conducted in the last week of April 2018 and included any publications (published between 2000 and 2018) that matched the search phrases listed above. After excluding publications based on relevance (title and abstract only), we ended up with an initial collection of 65 publications.

### Qualitative data analysis: Phase 1

These publications (65) were subsequently imported into a qualitative data analysis software (QDAS) package called Atlas.ti to quantify the qualitative data (i.e. selected publications). Atlas.ti performs analyses of textual data by associating pieces of text (*quotes* in Atlas.ti) with one or more *codes*. Within the context of Atlas.ti, codes are short phrases that can be used to logically group one or more quotes from a variety of textual sources (called *documents* in Atlas.ti). For example, the code called ++*qdas:limitations* was used to logically group quotes from a number of textual data sources (publications in this context). Using QDAS packages in this manner allowed us to collectively analyse a large set of data in a structured manner. This often leads to the discovery of latent themes (Albertus, Ngwenyama & Brown 2015). In addition to the discovery of latent themes, we also focused on identifying areas of theoretical overlap (called *co-occurrence* in Atlas.ti). This was achieved by visualising the codes (Hwang 2008; Knigge & Cope 2006) and their associated quotes in such a manner that we were able to see the instances of co-occurrence on an Atlas.ti *network*, as illustrated in Figure 1.

For example, the code *findings:awareness* is coded in such a manner that it *co-occurs* with the code *findings:personality influence on behaviour*. Here, the quote (labelled 24:23) is associated with both of the aforementioned codes. The same applies to quote 24:27. These areas of overlap in turn allowed us to identify theoretical relations, which led to the creation of our propositions. For example, Figure 1 was used to support the proposition that awareness influences behaviour. Additionally, such a structured approach enabled us to create

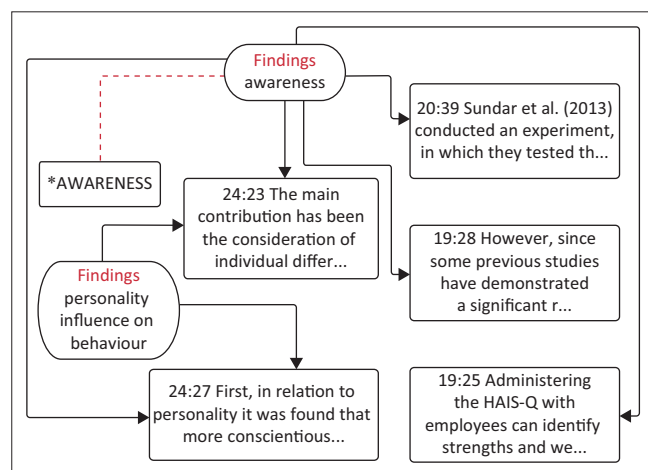


FIGURE 1: Example of co-occurrence in Atlas.ti.

synthesised narratives by combining multiple perspectives on a theme or code (Bandara, Miskon & Fieft 2011).

Although software packages, such as Atlas.ti and NVivo, facilitate analyses by providing a set of software functions to collate and code data, the onus is still on the researcher(s) to analyse and interpret the data (Paulus et al. 2017). In other words, QDAS packages should not overshadow the methodological approach by imposing software-specific behaviour, but rather complement it (Knigge & Cope 2006). For example, Bandara et al. (2011) suggest that researchers create an *a priori* coding framework before engaging with the software. To this end, we created our own coding framework by adding codes unique to our study to those suggested by Bandara et al. (2011).

Following this, all 65 publications were read in detail to ascertain whether they would be useful within the context of this article. This resulted in the exclusion of 30 publications (i.e. articles that are not relevant). After deciding on our final set of publications, we deductively coded the remainder of the publications by using the initial coding framework. This resulted in the creation of 827 coded quotes, which concluded phase 1 of the content analysis.

### Qualitative data analysis: Phase 2

Although the second phase of our content analysis still made use of the initial framework, its main focus was on coding for relevant content in an inductive manner. As such, certain codes were merged into what Atlas.ti calls *code groups* – henceforth referred to as *themes*. This process led to the discovery of additional themes which increased the number of coded quotes to 1360. In this manner, three themes were created, as guided by the study objectives, namely, *influence of awareness on behaviour*, *influence of personality on behaviour* and *use of theory*. Together, these three themes contained 36 merged codes and although this formed the focus of the study, a number of additional code groups were created. These additional groups assisted in the creation of a suitable introduction, literature review and provided support for certain arguments. Together, these code groups guided not only the theoretical development of the propositions but also the resultant narratives.

## Theoretical development and propositions

In this section, we first provide an outline of how the TPB (amongst others) has been used in related studies, followed by a two-part discussion detailing the development of the propositions to be evaluated.

### Use of behavioural theories

The TPB, an adapted version of the theory of reasoned action (TRA), suggests that an individual's intention to behave in a certain way is determined by three factors: attitude, subjective norms and perceived behavioural control

(Ajzen 1991). Within this context, attitude is defined as the extent to which an individual either positively or negatively values performing a behaviour. Thus, if a Facebook user displays a positive attitude towards sharing information (possibly unaware of surveillance), they may be more likely to use third-party apps (Taneja et al. 2014). Perceived behavioural control largely determines how likely an individual perceives himself or herself to execute the intended behaviour, as determined by the resources at their disposal. Such resources include any of the following combinations: information, beliefs about self-efficacy, time and money, amongst others (Tariq et al. 2017). Thus, if a Facebook user has access to the required resources to such an extent that he or she believes they are able to use third-party apps effectively, it will influence their intention to do so. Furthermore, given that an individual has access to the aforementioned resources and has a positive attitude towards the behaviour in question, subjective norms dictate an individual's perception about what others deem he or she should do (Jafarkarimi et al. 2016).

It is exactly this focus on general motivational factors that makes it possible to use this theory to assess the behavioural intent of any voluntary activity (Armitage & Conner 2001). In a study on cyber-slacking, Taneja et al. (2014) used TPB to evaluate students' intent to engage in this form of distracting behaviour and used the factors as described above. Their results indicated that both subjective and descriptive norms have a significant effect on a student's intent to participate in cyber-slacking. To better understand the antecedents that influence employees' attitudes towards information security policy compliance, Bulgurcu, Cavusoglu and Benbasat (2010) also adapted TPB by combining it with rational choice theory (RCT). In general, RCT explains the choices individuals make to achieve a specific goal (Taneja et al. 2014). Some authors, such as Hallam and Zanella (2017), have also suggested the use of construal level theory (CLT) to assist researchers in understanding the differences in users' perceived value of performing a behaviour. They argue that such a value-laden understanding may go a long way towards explaining the existence of the privacy paradox, which is defined as the difference between users' intended and actual privacy-related behaviour. Other theories, such as cognitive deficiency theory (CDT), make the argument that it is not the value of privacy outcomes, but rather the lack of privacy protection knowledge that determines behaviour (Hallam & Zanella 2017). However, according to Gordon (2004), CDT cannot adequately explain why the so-called knowledgeable users (those working in the IT industry) perpetuate information privacy beliefs that tilt the scales in favour of the privacy paradox.

As opposed to specifying the motivational factors upfront, certain theories such as the uses and gratification theory (UGT) attempt to understand the needs and associated motives for making use of media (Lee et al. 2016). Hence, Lee et al. (2016) used this theory to evaluate the influence of previously determined motives such as social relations, interactions, time management, entertainment value, self-expression and purpose. Although Lee et al. made specific reference to individual differences (such as personality types), their focus

on identifying rather than using motivational factors made it unsuitable in the context of this article. The same holds for theories that evaluate trust, such as the socio-cognitive theory (SCT), which Wang and Drake (2015) used to understand the relationship between job applicants and placement agencies.

To calculate the likelihood of performing a specific behaviour, authors have also made use of privacy calculus. In essence, privacy calculus argues that a user will assess the risks of performing a behaviour in relation to the benefits. When viewed in the context of exchanging personal information, a user may elect to share such information with the understanding that he or she will receive something in return. Therefore, users are making a rational choice based solely on the aforementioned benefit and risk assessment (Li et al. 2015). Although privacy calculus will give some insights as to why users make use of third-party apps (their perceived benefit), it does not take awareness or personality types into account. Similarly, concerns for information privacy (CFIP) theory primarily considers the privacy of personal information from an organisational perspective (Kusyanti et al. 2017). As such, CFIP would not adequately capture factors such as attitude and awareness. The same applies to the use of Internet users' information privacy concerns (IUIPC), as applied by Kusyanti et al. (2017) in their study on teens' information privacy concerns. Although Jiang et al. (2016) used TPB, they did so within a Chinese microblogging environment with a specific interest in the effect of self and social identity on behavioural intent.

## The influence of personality type

Several authors have used a variety of theoretical perspectives and personality tests to further academic efforts in this area (Shropshire, Warkentin & Sharma 2015; Wang et al. 2015; Xu et al. 2016). One such personality test is called the Big Five. We selected the Big Five not only because of its widespread acceptance as a valid and reliable model (Barrick, Mount & Judge 2001) but also because it is considered a good indicator of Internet use (Devaraj, Easley & Crant 2008). The Big Five consists of five personality types: *conscientiousness*, *agreeableness*, *openness to experience*, *neuroticism* and *extraversion*. It is generally accepted that these personality types influence not only decision-making but also, importantly, behaviour (Amichai-Hamburger, Wainapel & Fox 2002). For example, it has been found that certain personality types within the Big Five (conscientiousness and agreeableness) are prone to less risky behaviour (Skues, Williams & Wise 2012).

*Conscientious* individuals are characterised as organised, careful, hardworking, persistent and reliable, possessing an innate desire to succeed (James et al. 2017; Pentina et al. 2016). This is mirrored in a study on the use of mobile leisure apps, where the authors confirmed that conscientious individuals are less likely to make use of them as these apps are viewed as a hindrance to the pursuit of success (Xu et al. 2016).

Individuals high in *agreeableness* are often considerate and display high levels of self-control, compliance and trust

(Koban et al. 2018; Shropshire et al. 2015). Studies have found that such users not only disclose less personal information but also make use of fewer social media security features (Koban et al. 2018). Moreover, users high in agreeableness are more likely to adopt security software and possess greater concern for the security of their personal information (McCormac et al. 2017).

On the contrary, individuals high in *openness to experience* use their imagination, have a wide array of interests and make use of newer technologies (Amichai-Hamburger & Vinitzky 2010; Skues et al. 2012). As such, they are often characterised as early adopters of social media, prefer to experiment and are adept at avoiding risk (Shropshire et al. 2015).

*Neurotic* individuals tend to experience higher levels of emotional stress and anxiety (Koban et al. 2018; Pentina et al. 2016). They also tend to use technology to avoid social contact and rather engage with other individuals in a technological manner (Shropshire et al. 2015). It has also been found that individuals high in neuroticism are less likely to use Facebook with the intent to share personal information. However, when such individuals post information, they prefer to make use of features that facilitate various levels of control, such as posting on a Facebook wall (Skues et al. 2012). It is thus likely that neurotic individuals may adopt a positive attitude to third-party apps, as they are likely to share personal information on social media.

Individuals high in *extraversion* are typically more sociable, outgoing, affectionate and talkative (Warkentin et al. 2012). They prefer the company of others, and although such individuals may like others, they are not always likeable (James et al. 2017). It is these traits that cause extroverted individuals to take more risks (McCormac et al. 2017).

### The behavioural influence of personality

Literature makes specific reference to studies where other researchers have also endeavoured to measure the influence of personality types. For example, Guido, Capestro and Peluso (2007) found that introverted individuals are more likely to do shopping as a utilitarian exercise, as opposed to the hedonic shopping behaviour of individuals high in extraversion. Although neuroticism and extraversion are considered direct opposites, Gohary and Hanzee (2014) found that they both exhibit hedonic behaviour when shopping. Another area that has been explored using personality types is cybersecurity compliance (Bulgurcu et al. 2010) and training, where researchers have provided evidence that individuals who exhibit high levels of conscientiousness and agreeableness are more likely to display compliant behaviour. To further this argument, Warkentin et al. (2012) conducted a survey to understand how these personality types influence threat and coping appraisal, as well as their perspective on sanctions. Their results indicate that individuals behave differently in similar conditions, which suggests that effective cybersecurity training should take such differences into account if it is to be

truly effective. From the evidence provided, it is thus plausible that an individual's personality type influences his or her behaviour. We therefore propose the following:

**Proposition 1:** An individual's personality type will influence his or her intent to make use of third-party apps on Facebook.

### The influence of awareness

In this article, we argue that an individual's awareness of SMS influences his or her intent to make use of third-party Facebook apps. We define SMS as the monitoring and capturing of personal information when making use of social media-based third-party apps – Facebook in particular. From the literature it is known that although organisations believe information security awareness is important, they openly admit that not enough resources are allocated to furthering such efforts (Krugger & Kearney 2006). Moreover, those organisations that conduct awareness training do not adequately address individual differences (including personality), which ultimately influence information security behaviour. For example, when individuals are faced with the decision to comply with an organisation's information security policy (ISP), it has been found that awareness directly influences not only their beliefs on the possible outcomes, but more importantly their attitude towards compliance (Tsohou, Karyda & Kokolakis 2015), thus acting as an antecedent of their intent to comply. In a similar study on privacy behaviour in students, Van Schaik et al. (2018) found that although there was little relation between their privacy attitudes and the information they shared on Facebook, users were concerned that the shared information could be identified.

Other studies have found that individuals' incorrect assumptions about information security are indicative of the role played by information security awareness and trust (Van der Schyff & Krauss 2014). In such instances, individuals cited that they were not knowledgeable enough to make informed information security decisions.

However, awareness of privacy settings alone has been shown to have no effect on how information is provisioned, as younger adults tend to assume that the necessary legal structures are in place to protect their personal information (Miltgen & Peyrat-Guillard 2014). In a similar study, Junger, Montoya and Overink (2017) found that users make a number of assumptions as to what type of information cybercriminals find appealing. For example, in the experiments they conducted, many of the users did not understand how the information they were asked to provide (an email address) could be misused in a phishing campaign.

When individuals are equipped with sufficient knowledge (and are thus more aware), their attitude towards information security improves. One example is the study conducted by Mamonov and Benbunan-Fich (2018) where the authors found a positive increase in the attitudes of individuals towards password strength. Similar effects in the attitude

towards information security are reported by Karwatzki et al. (2017), who found that an increase in transparency features (thus raising awareness) had a positive influence on information security behaviour, with users sharing less personal information. Conger, Pratt and Loch (2013) provide a similar argument, stating that individuals are likely to change their security behaviour once they become aware of the extent of secondary data use. We therefore propose the following:

**Proposition 2:** An individual's information security awareness of SMS will positively influence his or her attitude towards the use of third-party Facebook apps.

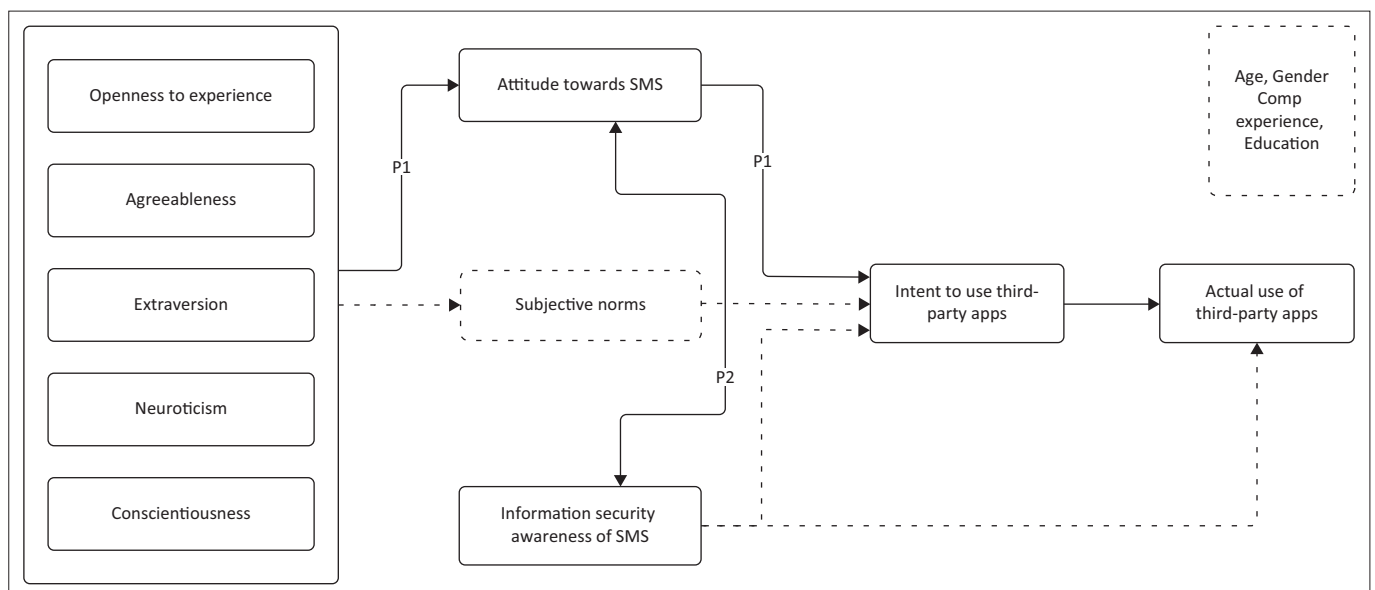
## Discussion

In Figure 2, we illustrate our research model – an adapted version of the TPB. We specifically replaced the construct *perceived behavioural control* with *information security awareness of SMS* for which we provide support in the previous section (as per Proposition 2). In this model, the five personality types take the form of independent variables, with *information security awareness of SMS* and *attitude towards SMS* acting as moderating variables. Together, both the independent and moderating variables influence the dependent variable, namely, *actual use of third-party apps*. Note that this article does not provide arguments for the inclusion of the construct named *subjective norms*. We also omit arguments for the link between *information security awareness of SMS* and *intent to use third-party apps*. Together, these form part of the limitations of this article.

This research model allows one to evaluate the influence of a user's personality type on his or her attitude towards using third-party apps on Facebook. This corresponds to the first proposition which is illustrated as P1 in Figure 2. Because attitude influences behavioural intent (as per TPB) and the first proposition wishes to evaluate the influence of personality types on a user's intent to use third-party apps,

we have aligned this relationship with P1. In this regard, our content analysis suggests that conscientious users are one of the most important personality types to evaluate – mostly because of their cautious nature (Shropshire et al. 2015). Conscientious Facebook users are thus less likely to use third-party apps unless they are fully aware of their impact on the security of their personal information. Even when they are fully aware, such users may elect not to use certain third-party apps. In turn, this makes them the least susceptible to SMS. The same applies to agreeable users who display high levels of concern for the security of their personal information and are thus likely to adopt a cautious attitude towards the use of third-party apps on Facebook. As conscientious and agreeable users become more aware of the information security implications of SMS when making use of third-party apps, they are likely to re-evaluate their attitude towards SMS in general.

As awareness is not usually part of the TPB, substituting it for perceived behavioural control warrants some explanation. Theoretically, perceived behavioural control is defined as the relative ease of performing a specific behaviour. As such, it is considered to be an important predictor of behavioural intent. One might ask on which information or factors individuals rely when making such an assessment. We argue that one such means of attaining said information is by educating individuals about the risks of disclosing personal information on social networks in general and third-party apps in particular. It is exactly this lack of expertise that affects security-unaware individuals (Siponen 2001). It is thus possible that an educated individual (cybersecurity specific) will find it easier to effectively manage and make decisions related to the security of his or her personal information accessed via third-party apps. Even knowledge acquired from one's circle of influence could sufficiently educate an individual and thus increase self-efficacy (Heinze 2008). Given that extant research suggests that anxiousness



SMS, Social media surveillance.

**FIGURE 2:** Research model.

influences individuals' motivation to act on their level of self-efficacy, one could posit that neurotic individuals will most likely perceive themselves as ineffective at managing the security of their personal information. This may make them rely more on the default security settings when making use of third-party apps, as any changes made by themselves might be perceived as incorrect or insecure.

Conversely, confident individuals (i.e. extroverts) are most likely to perceive the ease of securing their personal information as a trivial matter. If the central tenet of awareness within this context is education, it might be beneficial to also consider academic performance (i.e. appetite for learning). For example, De Feyter et al. (2012) found that agreeableness has a positive influence on academic performance. Given that these individuals place a strong emphasis on what others think and that learning increases awareness, it is plausible that those individuals high in agreeableness will exhibit higher levels of security awareness. In turn, if significant others display a positive attitude towards SMS, these agreeable individuals' level of awareness may also positively influence their attitude towards SMS.

On the other hand, low levels of emotional stability – especially amongst women and younger individuals – often lead to the increased use of not only Facebook but also the Internet as a whole (Amichai-Hamburger & Ben-Artzi 2003). These individuals need to both control information and feel a sense of belonging. This is important, as it furthers the argument that personality exerts a behavioural influence in general online, which may extend to the use of third-party apps in particular. Let us consider the use of Spotify (a music streaming app) by neurotic Facebook users (i.e. they have logged on with their Facebook credentials). The aforementioned users are likely to continue using the app not only because they are influenced by others who think they should use it, but also because they are able to 'follow' other users via play-lists and thus feel a sense of belonging. Being aware that their personal information is accessible by Facebook may only be an issue if they are sufficiently educated (thus aware); however, theory suggests that the aforementioned sense of belonging and the need of self-assurance are core (even overriding) individual differences within neurotic individuals. As such, awareness may influence attitude to a lesser extent amongst these individuals. The influence of awareness within the context of this article corresponds to the second proposition (P2), as illustrated in Figure 2.

Evaluating these propositions will allow organisations to modify existing security education training and awareness (SETA) campaigns to take the personality types of users into account. For example, training efforts could be tailored to focus more on users that display higher levels of extraversion, and openness to experience who have a higher propensity to take risks on and explore Facebook rather than first gaining some knowledge (and thus becoming more aware) regarding activities, such as SMS. From a practical perspective, this research model could also be used on other platforms, such as those provided by Google. Corporates that wish to increase

levels of consumer trust could incorporate these results in the descriptions of the apps they offer so as to aid transparency. Given that individuals are usually aware of their personality type (Gosling, Rentfrow & Swann 2003), a raised level of awareness with regard to SMS would allow them to make an informed decision when selecting third-party apps on Facebook.

## Limitations

The approach outlined in this article is limited on three fronts. Firstly, the codes and subsequent interpretations are influenced by the researchers' own thoughts and worldviews on the topic of SMS. As such, other researchers' models on the same topic may differ based on their views. For example, some researchers may view the value of information to be of particular importance and thus elect to rather use privacy calculus as opposed to the TPB. Secondly, because this study used a structured approach, the resultant inductively deduced model is based on a specific subset of literature. It stands to reason that a different search string (thus subset) may have also influenced the resultant analysis. Thirdly, we only provided arguments to support the links between a portion of the constructs contained in the full TPB and not all the relationships from the original model are illustrated. For example, the link between *information security awareness of SMS* and *intent to use third-party apps* is not argued here because of space concern.

## Conclusion

In this article, we argued that both personality types and awareness influence behaviour. Using a structured approach, we selected a number of publications that explored behavioural aspects of information security. These publications were coded in two phases, leading to the identification of three main themes. From these themes we derived two propositions, which were used in our research model – an adapted version of the TPB.

Our research model makes use of *information security awareness of SMS* instead of *perceived behavioural control*; therefore, future research is required to explore the influence of both attitude and subjective norms. Similarly, researchers could also evaluate the influence of individual cultural differences instead of personality types by adopting an approach similar to that of Srite and Karahanna (2006). In addition to the influence of culture and personality, more work is required to ascertain the influence of value, responsibility, assumption and ignorance from a South African perspective. Moreover, such research should not only illustrate theory development but also make inferences based on empirical data.

## Acknowledgements

### Competing interests

The views expressed in this article are that of the authors and not an official position of Rhodes University.

## Author's contributions

The corresponding author (K.V.D.S.) selected, read and coded the publications after receiving conceptual input from the second author (S.F.). Following this, both authors worked on the resultant text and research model. Further refinements to the conceptual model were suggested by the second author, nearing completion of the article.

## References

- Ajzen, I., 1991, 'The theory of planned behavior', *Organizational Behavior and Human Decision Processes* 50, 179–211. [https://doi.org/10.1016/0749-5978\(91\)90020-T](https://doi.org/10.1016/0749-5978(91)90020-T)
- Albertus, R., Ngwenyama, O. & Brown, I., 2015, 'A critical discourse analysis of governance issues affecting public private partnership contracting for information systems implementations: A South African case study', *SAICSIT'15*, ACM, 28–30th September, pp. 1–10.
- Amichai-Hamburger, Y. & Ben-Artzi, E., 2003, 'Loneliness and Internet use', *Computers in Human Behavior* 19(1), 71–80. [https://doi.org/10.1016/S0747-5632\(02\)00014-6](https://doi.org/10.1016/S0747-5632(02)00014-6)
- Amichai-Hamburger, Y. & Vinitzky, G., 2010, 'Social network use and personality', *Computers in Human Behavior* 26(6), 1289–1295. <https://doi.org/10.1016/j.chb.2010.03.018>
- Amichai-Hamburger, Y., Wainapel, G. & Fox, S., 2002, "'On the Internet no one knows I'm an introvert": Extroversion, neuroticism, and Internet interaction', *Cyber Psychology & Behavior* 5(2), 125–128. <https://doi.org/10.1089/109493102753770507>
- Armitage, C.J. & Conner, M., 2001, 'Legacy of the Theory of Planned Behaviour: A meta-analytic review', *British Journal of Social Psychology* 40(1), 471–499. <https://doi.org/10.1348/014466601164939>
- Bandara, W., Miskon, S. & Fietl, E., 2011, 'A systematic, tool-supported method for conducting literature reviews in IS', *Information Systems Journal* 1–14.
- Barrick, M.R., Mount, M.K. & Judge, T.A., 2001, 'Personality and performance at the beginning of the new millennium: What do we know and where do we go next?', *International Journal of Selection and Assessment* 9(1&2), 9–30. <https://doi.org/10.1111/1468-2389.00160>
- Barth, S. & de Jong, M.D.T., 2017, 'The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review', *Telematics and Informatics* 34(7), 1038–1058. <https://doi.org/10.1016/j.tele.2017.04.013>
- Bulgurcu, B., Cavusoglu, H. & Benbasat, I., 2010, 'Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness', *MIS Quarterly* 34(3), 523–548. <https://doi.org/10.2307/25750690>
- Chang, C.W. & Chen, G.M., 2014, 'College students' disclosure of location-related information on Facebook', *Computers in Human Behavior* 35, 33–38. <https://doi.org/10.1016/j.chb.2014.02.028>
- Chen, R., Sharma, S.K. & Rao, R., 2016, 'Members' site use continuance on Facebook: Examining the role of relational capital', *Decision Support Systems* 90, 86–98. <https://doi.org/10.1016/j.dss.2016.07.001>
- Confessore, N., 2018, 'Cambridge Analytica and Facebook: The scandal and the fallout so far', *The New York Times*, 04 March, viewed 18 July 2018, from <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>.
- Conger, S., Pratt, J.H. & Loch, K.D., 2013, 'Personal information privacy and emerging technologies', *Information Systems Journal* 23(5), 401–417. <https://doi.org/10.1111/j.1365-2575.2012.00402.x>
- Devaraj, S., Easley, R.F. & Crant, J.M., 2008, 'Personality matter? Relating the five-factor model to technology acceptance', *Information Systems Research* 19(1), 93–105. <https://doi.org/10.1287/isre.1070.0153>
- De Feyter, T., Caers, R., Vigna, C. & Berings, D., 2012, 'Unraveling the impact of the Big Five personality traits on academic performance: The moderating and mediating effects of self-efficacy and academic motivation', *Learning and Individual Differences* 22(4), 439–448. <https://doi.org/10.1016/j.lindif.2012.03.013>
- Fuchs, C., 2012, 'Political economy and surveillance theory', *Critical Sociology* 39(5), 671–687. <https://doi.org/10.1177/0896920511435710>
- Gohary, A. & Hanzaae, K.H., 2014, 'Personality traits as predictors of shopping motivations and behaviors: A canonical correlation analysis', *Arab Economic and Business Journal* 9(2), 166–174. <https://doi.org/10.1016/j.aebj.2014.10.001>
- Gordon, S., 2004, *Privacy: A study of attitudes and behaviors in US, UK and EU information security professionals*, viewed 19 July 2018, from <http://www.symantec.com/avcenter/reference/privacy.attitudes.behaviors.pdf>.
- Gosling, S.D., Rentfrow, P.J. & Swann, W.B., 2003, 'A very brief measure of the Big-Five personality domains', *Journal of Research in Personality* 37(6), 504–528. [https://doi.org/10.1016/S0092-6566\(03\)00046-1](https://doi.org/10.1016/S0092-6566(03)00046-1)
- Green, D. & Hanbury, M., 2018, *If you shopped at these 15 stores in the last year, your data might have been stolen*, viewed 19 July 2018, from <http://www.businessinsider.com/data-breaches-2018-4?IR=T>.
- Guido, G., Capestro, M. & Peluso, A.M., 2007, 'Experimental analysis of consumer stimulation and motivational states in shopping experiences', *International Journal of Market Research* 49(3), 365–386. <https://doi.org/10.1177/147078530704900307>
- 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>
- Heinze, N.D., 2008, 'Why college undergraduates intend to pursue the information technology major: A multi-theoretical perspective', *Dissertation Abstracts International Section A: Humanities and Social Sciences* 68(11–A), viewed 18 July 2018, from <http://proxygw.wrlc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=psyh&AN=2008-99091-162&site=eds-live&scope=site>.
- Hwang, S., 2008, 'Utilizing qualitative data analysis software', *Social Science Computer Review* 26(4), 519–527. <https://doi.org/10.1177/0894439307312485>
- JafarKarimi, H., Saadatdoost, R., Sim, A.T.H. & Hee, J.M., 2016, 'Behavioral intention in social networking sites ethical dilemmas: An extended model based on theory of planned behavior', *Computers in Human Behavior* 62, 545–561. <https://doi.org/10.1016/j.chb.2016.04.024>
- James, T.L., Lowry, P.B., Wallace, L. & Warkentin, M., 2017, 'The effect of belongingness on obsessive-compulsive disorder in the use of online social networks', *Journal of Management Information Systems* 34(2), 560–596. <https://doi.org/10.1080/07421222.2017.1334496>
- Jeong, Y. & Kim, Y., 2017, 'Privacy concerns on social networking sites: Interplay among posting types, content, and audiences', *Computers in Human Behavior* 69, 302–310. <https://doi.org/10.1016/j.chb.2016.12.042>
- Jiang, C., Zhao, W., Sun, X., Zhang, K., Zheng, R. & Qu, W., 2016, 'The effects of the self and social identity on the intention to microblog: An extension of the theory of planned behavior', *Computers in Human Behavior* 64, 754–759. <https://doi.org/10.1016/j.chb.2016.07.046>
- Jordaan, Y. & Van Heerden, G., 2017, 'Online privacy-related predictors of Facebook usage intensity', *Computers in Human Behavior* 70, 90–96. <https://doi.org/10.1016/j.chb.2016.12.048>
- Junger, M., Montoya, L. & Overink, F.J., 2017, 'Priming and warnings are not effective to prevent social engineering attacks', *Computers in Human Behavior* 66, 75–87. <https://doi.org/10.1016/j.chb.2016.09.012>
- Karwatzki, S., Dytynko, O., Trenz, M. & Veit, D., 2017, 'Beyond the personalization–Privacy Paradox: Privacy valuation, transparency features, and service personalization', *Journal of Management Information Systems* 34(2), 369–400. <https://doi.org/10.1080/07421222.2017.1334467>
- Knigge, L.D. & Cope, M., 2006, 'Grounded visualization: Integrating the analysis of qualitative and quantitative data through grounded theory and visualization', *Environment and Planning A* 38(11), 2021–2037. <https://doi.org/10.1068/a37327>
- Koban, K., Stein, J.P., Eckhardt, V. & Ohler, P., 2018, 'Quid pro quo in Web 2.0. Connecting personality traits and Facebook usage intensity to uncivil commenting intentions in public online discussions', *Computers in Human Behavior* 79, 9–18. <https://doi.org/10.1016/j.chb.2017.10.015>
- Kruger, H.A. & Kearney, W.D., 2006, 'A prototype for assessing information security awareness', *Computers and Security* 25(4), 289–296. <https://doi.org/10.1016/j.cose.2006.02.008>
- 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/10.1016/j.procs.2017.12.199>
- Lee, S.Y., Hansen, S.S. & Lee, J.K., 2016, 'What makes us click like on Facebook? Examining psychological, technological, and motivational factors on virtual endorsement', *Computer Communications* 73, 332–341. <https://doi.org/10.1016/j.comcom.2015.08.002>
- Li, K., Lin, Z. & Wang, X., 2015, 'An empirical analysis of users' privacy disclosure behaviors on social network sites', *Information and Management* 52(7), 882–891. <https://doi.org/10.1016/j.im.2015.07.006>
- Lyon, D., 2014, 'Surveillance, Snowden, and Big Data: Capacities, consequences, critique', *Big Data & Society* 1(2), 1–13. <https://doi.org/10.1177/2053951714541861>
- Mamonov, S. & Benbunan-Fich, R., 2018, 'The impact of information security threat awareness on privacy-protective behaviors', *Computers in Human Behavior* 83, 32–44. <https://doi.org/10.1016/j.chb.2018.01.028>
- McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M. & Pattinson, M., 2017, 'Individual differences and information security awareness', *Computers in Human Behavior* 69, 151–156. <https://doi.org/10.1016/j.chb.2016.11.065>
- Miltgen, C.L. & Peyrat-Guillard, D., 2014, 'Cultural and generational influences on privacy concerns: A qualitative study in seven European countries', *European Journal of Information Systems* 23(2), 103–125. <https://doi.org/10.1057/ejis.2013.17>
- Moore, K. & McElroy, J.C., 2012, 'The influence of personality on Facebook usage, wall postings, and regret', *Computers in Human Behavior* 28(1), 267–274. <https://doi.org/10.1016/j.chb.2011.09.009>
- Paulus, T., Woods, M., Atkins, D.P. & Macklin, R., 2017, 'The discourse of QDAS: Reporting practices of ATLAS.ti and NVivo users with implications for best practices', *International Journal of Social Research Methodology* 20(1), 35–47. <https://doi.org/10.1080/13645579.2015.1102454>
- 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>
- Shropshire, J., Warkentin, M. & Sharma, S., 2015, 'Personality, attitudes, and intentions: Predicting initial adoption of information security behavior', *Computers and Security* 49, 177–191. <https://doi.org/10.1016/j.cose.2015.01.002>
- Siponen, M., 2001, '5 Dimensions of Information Security Awareness', *ACM SIGCAS Computers and Society* 31(2), 24–29. <http://doi.org/10.1145/503345.503348>



- Skues, J.L., Williams, B. & Wise, L., 2012, 'The effects of personality traits, self-esteem, loneliness, and narcissism on Facebook use among university students', *Computers in Human Behavior* 28(6), 2414–2419. <https://doi.org/10.1016/j.chb.2012.07.012>
- Srite, M. & Karahanna, E., 2006, 'The role of espoused national cultural values in technology acceptance', *MIS Quarterly* 30(3), 679–704. <https://doi.org/10.2307/25148745>
- 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 and Security* 77, 179–208. <https://doi.org/10.1016/j.cose.2018.03.015>
- Taneja, A., Vitrano, J. & Gengo, N.J., 2014, 'Rationality-based beliefs affecting individual's attitude and intention to use privacy controls on Facebook: An empirical investigation', *Computers in Human Behavior* 38, 159–173. <https://doi.org/10.1016/j.chb.2014.05.027>
- Tariq, J., Sajjad, A., Usman, A. & Amjad, A., 2017, 'The role of intentions in facebook usage among educated youth in Pakistan: An extension of the theory of planned behavior', *Computers in Human Behavior* 74, 188–195. <https://doi.org/10.1016/j.chb.2017.04.045>
- Tsohou, A., Karyda, M. & Kokolakis, S., 2015, 'Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs', *Computers and Security* 52, 128–141.
- Van Schaik, P., Jansen, J., Onibokun, J., Camp, J. & Kusev, P., 2018, 'Security and privacy in online social networking: Risk perceptions and precautionary behaviour', *Computers in Human Behavior* 78, 283–297. <https://doi.org/10.1016/j.chb.2017.10.007>
- Van der Schyff, K. & Krauss, K., 2014, 'Higher Education Cloud Computing in South Africa: Towards understanding trust and adoption issues', *South African Computer Journal* 55(1), 40–55. <https://doi.org/10.18489/sacj.v55i0.254>
- Vladlena, B., Saridakis, G., Tennakoon, H. & Ezingard, J.N., 2015, 'The role of security notices and online consumer behaviour: An empirical study of social networking users', *International Journal of Human Computer Studies* 80, 36–44.
- Wagner, A., Wessels, N., Buxmann, P. & Krasnova, H., 2018, 'Putting a price tag on personal information – A literature review', *Proceedings of the 51st Hawaii International Conference on System Sciences*, pp. 3760–3769, viewed 25 February 2018, from <https://scholarspace.manoa.hawaii.edu/bitstream/10125/50362/1/paper0475.pdf>.
- Wang, Y., Sun, S., Drake, J.R. & Hall, D., 2015, 'Job applicants' information privacy-protective response: Exploring the roles of technology readiness and trust job applicants' information privacy-protective response: Exploring the roles of technology readiness and trust', *Twenty-first Americas Conference on Information Systems (AMCIS) 2015 Proceedings*, Puerto Rico, August, 2015, pp. 1–13. <http://doi.org/10.13140/RG.2.1.4486.2887>
- Warkentin, M., McBride, M., Carter, L., Johnston, A. & Johnston, A.C., 2012, 'The role of individual characteristics on insider abuse intentions', viewed n.d., from <http://aisel.aisnet.org/amcis2012%0Ahttp://aisel.aisnet.org/amcis2012/proceedings/ISSecurity/28%0Ahttp://aisel.aisnet.org/amcis2012%0Ahttp://aisel.aisnet.org/amcis2012/proceedings/ISSecurity/28>.
- Xu, R., Frey, R.M., Fleisch, E. & Ilic, A., 2016, 'Understanding the impact of personality traits on mobile app adoption – Insights from a large-scale field study', *Computers in Human Behavior* 62, 244–256. <https://doi.org/10.1016/j.chb.2016.04.011>