RHODES UNIVERSITY

Where leaders learn

A PERSONALITY-BASED SURVEILLANCE MODEL FOR FACEBOOK APPS

by

Karl van der Schyff

A PERSONALITY-BASED SURVEILLANCE MODEL FOR FACEBOOK APPS

by

Karl van der Schyff
12V7031

THESIS

submitted in fulfilment of the requirements for the degree

DOCTOR OF PHILOSOPHY

in

INFORMATION SYSTEMS

in the

FACULTY OF COMMERCE

of

RHODES UNIVERSITY

Supervisor: **Prof. Stephen Flowerday**

November 2019

ABSTRACT

The surveillance of data through the use of Facebook Apps is an ongoing and persistent problem that impacts millions of users. Nonetheless, limited research has been conducted investigating to what extent a Facebook user's personality influences their awareness of such surveillance practices. Thus, to understand this situation better, the current study inductively developed four propositions from secondary data sources as part of a detailed content analysis. Spanning three search and analysis phases the content analysis led to the development of the research model. Guided by the propositions and research questions, a questionnaire was developed based on the relevant constructs prescribed by the Theory of Planned Behaviour. This questionnaire was used, and a total of 651 responses were collected from Facebook users over the age of 18 years old and residing in the United States of America. Primary data took place at both a univariate and multivariate level with a specific focus on the development of a structural model. Interpretation of the structural model revealed that out of all the Big Five personality traits, Conscientiousness exhibited the strongest relationship with information security awareness followed by Openness to Experience and Neuroticism, respectively. The results further indicated that the model constructs based on attitude, social norms and awareness significantly influenced the intended use of Facebook Apps. The study also contributes by indicating which personality traits are most vulnerable to Facebook App surveillance. For example, it was found that individuals high in Conscientiousness are the least vulnerable with individuals high in Extraversion being the most vulnerable. Since the results indicate that not all the personality traits are significantly related to the model constructs, additional factors may contribute to App surveillance in this context. Concerning this, factors such as user apathy, information privacy, privacy concerns, control and Facebook dependency are discussed as a means to argue why this might be the case.

DECLARATION

I ...., hereby declare that:

- The work in this thesis is my own work.
- All sources used or referred to have been documented and recognised.
- This thesis has not previously been submitted in full or partial fulfilment of the requirements for a qualification.
- I am fully aware of Rhodes University's policy on plagiarism and I have taken every precaution to comply with the regulation.
- Ethics number is CIS18-10

....

Date:

ACKNOWLEDGEMENTS

Firstly, thanks to Prof. Flowerday for all his support. Without you this would not have been possible. Secondly, thanks to my family who sacrificed a lot during the development of this thesis.

GLOSSARY

Term	Definition
Attitude	A positive or negative evaluation of an object of thought (Bohner & Wanke, 2002).
Descriptive norms	The perceptions of what others are doing within context (Benson et al., 2015).
Facebook App surveillance	The harvesting or secondary use of Facebook-based personal information captured while making use of Facebook-authored or third-party Facebook Apps.
Information security awareness	Within the context of this study this entails being aware of the risks when disclosing personal information on Facebook or Facebook Apps.
Social norms	An umbrella term that includes descriptive, subjective, and injunctive norms. These norms are said to influence the formation of beliefs that emerge from the interactions between members of a social group (Lapinski & Rimal, 2005). Note that injunctive norms are not evaluated in this study.
Subjective norms	The beliefs of others' approval of a behaviour (Chandran & Aleidi, 2018).
The Big Five	An established set of five personality traits used in this study (John & Srivastava, 1999). Using the Big Five Inventory, individuals are classified under the following five traits: Openness to Experience, Conscientiousness, Extraversion, Agreeableness, and Neuroticism. Note that these traits are not mutually exclusive, which means that it is possible for an individual to possess different levels of each. It is this resultant combination which form an individual's personality.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Chapter 1

INTRODUCTION

> "Every secret of a writer's soul, every experience of his life, every quality of his mind is written large in his works."
>
> — Virginia Woolf

This chapter provides a complete overview of this study by outlining not only the problem statement, objectives and research questions, but also the methodological approach. The reader is also presented with this study's theoretical contribution namely, a personality-based surveillance model for Facebook App users.

1.1 Background information

Although the surveillance of data has been taking place for decades, mainstream publicity as to the misuse of the surveilled personal information has only recently received extensive publicity. First amongst these is that of the Snowden revelations (circa 2013). As part of several interviews with The Guardian, Snowden not only disclosed detailed information about the mass surveillance conducted by several first-world countries (including the US) but he also admitted in a later interview that several social media corporates regularly funnel data to the National Security Agency (NSA) (Snowden, 2016). More information regarding the specific surveillance sources is provided by Michael Hayden (a former NSA director) who explicitly stated that although government agencies gather their surveillance data, much of it is also initially collected by corporates and merely redirected to intelligence agencies, such as the NSA (Hayden, 2014). Hayden specifically mentions Google, Yahoo, and Microsoft, although Facebook has also been implicated as a source of surveillance data.

With many of the social media platforms, such as Facebook and Twitter emphasising sharing and connecting these applications have become essential resources for users to form relationships by sharing information (Rosamond, 2015). Additionally, many Internet users participate in social networking as part of their daily routine (Hallam & Zanella, 2017). Such participation not only allows users to share content with friends and family, but also to accumulate social capital while developing in a psychosocial nature (Chen et al., 2016). With more than two billion active users, Facebook, and social networks in general, have become lucrative commercial environments for businesses, due to their ability to market to a broad captive audience with relative ease (Lam et al., 2019). For example, targeted advertising no longer relies on the completion of lengthy and time-consuming consumer surveys. Instead, corporates make use of Location-Based Services (LBS) to pinpoint the places users frequent. When combined with data related to a social media profile, social media corporates can create detailed descriptions of their users' behavioural patterns. Not only are the resultant data assemblages (a combination of location and profile data) useful for improving Facebook services, but they are also used as a commodity that is sold to third-party organisations (Fuchs, 2011).

However, these third-party organisations do not have to rely only on Facebook to create such data assemblages. Third parties could also develop Apps that users elect to access using their Facebook credentials - Facebook Apps within this context. This allows for the surveillance and the subsequent harvesting of user data through the linked App by utilising Application Programming Interfaces (APIs) (Koban et al., 2018). In this way, these third parties can combine the usage data of their App with the profile data on Facebook. A controversial example of this is the misuse of personal information by Cambridge Analytica. By determining the personality traits of Facebook users, Cambridge Analytica was able to gain insight into the likely voting behaviour of these users without their consent (Leetaru, 2018). In this case, a third-party App was developed (*thisisyourdigitallife*) with the intention of determining a user's personality traits. At least this is what the App's users were told (Symeonidis et al., 2018). However, unbeknownst to the user, this dataset was combined with their Facebook profile (they had to sign in with their Facebook credentials) and the resultant data assemblage, which also consisted of their friends' personal information, was misused.

From the brief discussion above, it would seem that social media corporates and third-party App developers have a lot to gain by studying the behaviour of their users. Not only is it useful to know when, where, and how these Apps are accessed, but also the personal information provided by users in order to use these Apps. For example, by studying the latter usage factors, it becomes possible to ascertain how likely it would be for a young female (and other demographic categories) to play Facebook games (also a type of App) and for how long. Given this information, it would also be possible to see which other Apps this user has linked to their profile. This type of metadata is of particular value to Facebook, since it allows them to sell advertising space to prospective clients who wish to target specific demographic sectors - in this case, young females, who happen to play Facebook-based games.

Moreover, since these Facebook Apps are now linked to the user's profile, they also have access to several pieces of personal information - information that is often used for purposes other than targeted advertising campaigns.

However, over and above the use of such demographic individual differences, there are also other means to ascertain user sentiment, and user attitude towards Apps. Some of which centres around the personality traits of these users. Since an individual's personality influences their behaviour (Ajzen, 2005) in addition to their attitude towards certain behaviour (Ajzen, 1991); it is plausible that a user's attitude towards their personal information influences their intent to use social media platforms. In turn, this determines what users willingly divulge on their social media profiles.

The availability of personal information on social media profiles benefits not only the social media platform, but also the third parties who misuse the information (Fuchs, 2017). For instance, companies such as Social Intelligence [1]do background checks of prospective employees by making use of social media-based personal information. Even the Facebook-based games such as Farmville are geared towards predictive analytics (Willson & Leaver, 2015). Importantly, none of these third parties made social media users aware of the extent to which the user's personal information was used. Cambridge Analytica even performed

[1] https://www.socialintel.com

analyses on shared information without the direct knowledge of the social media users in question (Pegg & Cadwalladr, 2018).

1.2 Problem statement

It is quite common to find media reports on breaches of social media-based personal information (Bronskill, 2019; Gordon & Ortutay, 2019). To illustrate the extent of this we refer readers to Figure 3.1 and 3.2 in Chapter Three. These breaches have not only led to financial losses (Li et al., 2015), but also to an increase in the concerns and the distrust expressed when sharing personal information on social media - a persistent matter that has been in the news for several years (Chakraborty et al., 2013; The Associated Press, 2019). It is not only because users have had negative experiences in this regard (Pentina et al., 2016), but also because they have become more aware and knowledgeable about privacy risks. In turn, some studies have indicated that this has made them suspicious of secondary information use when using these services (Bartsch & Dienlin, 2016).

Nevertheless, only 3% of the respondents in the latter study were able to correctly answer five questions about the online safety of their information (Pentina et al., 2016). Some studies argue that this is not only the result of privacy's abstract nature, but also because of its dependence on context. A lack of transparency and a lack of awareness as to how their personal information is used amplifies these matters (Hirschprung et al., 2016) - specifically, how personal information is to be used and by whom. Information from click-stream data to cloud-based files is indexed and harvested for a variety of reasons - one being the increase of capital (Conger et al., 2013).

However, even those individuals who have become more aware of the privacy risks, still maintain an attitude of indifference towards the privacy of personal information (Wisniewski et al., 2017). For Facebook users, such indifference stems not only from the complex nature of the privacy settings, but also because of the sense that the use of these settings is futile since the platform already has access to the information (Wisniewski et al., 2017). As such, users continue to make use of social media (Fatima et al., 2019), which makes them particularly vulnerable; not only because of said difficulty with using privacy settings, but also because these users naturally exhibit a wide variety of privacy behaviours.

This makes a single approach to privacy management problematic; especially if users are not only unaware of social media surveillance, but also of the extent to which their personal information is used once harvested through said surveillance practices (Srinivasan, 2019; Tsay-Vogel et al., 2018; Wisniewski et al., 2017).

In addition to the issues about privacy awareness, users are also unaware that Facebook analyses their profile information and preferences in order to extract individual traits. These traits are openly listed under the *Your ad preferences* page, yet 74% of users are unaware of this (Hitlin & Rainie, 2019). Furthermore, over half of the users who are aware of this expressed concern in this regard. Given that Facebook uses such trait-based analyses to predict an individual's online behaviour and that personality influences an individual's behaviour (Ajzen, 2005). The misuse and the exploitation of such individual differences is also problematic. As such, the central problem statement of this thesis is as follows;

> *Facebook users are unaware of the trait-based analyses and subsequent misuse of the personal information gathered when making use of Facebook Apps.*

Given that users continue their use of social media platforms amidst increased publicity of the privacy risks, it makes sense to evaluate their attitude towards the privacy of their personal information as a function of their level of information security awareness and the social norms that regulate the resultant behaviour (using the Theory of Planned Behaviour). To address the exploitation of the trait-based analyses mentioned above, it also makes sense to evaluate the influence of an individual's personality on attitude, social norms, and information security awareness; not so much because it is vital to identify the influences, but rather to understand to what extent they influence resultant behaviour.

1.3 Research questions

From the problem statement it follows that this study intends to evaluate the behavioural influence of a Facebook users' personality traits, attitude, social norms and information security awareness when using and sharing personal information via Facebook Apps.

To address the problem statement, the following main research question is put forward.

Main Question. *To what extent does the behaviour of certain Facebook users influence their use of Facebook Apps, given the misuse of personal information gathered through these Apps?*

To answer all the behavioural elements contained in the main research question, the following sub-questions were put forward:

- **Question One.** *To what extent does a Facebook user's attitude towards information privacy influence their intention to use Facebook Apps?* The aim of this question was to evaluate the first proposition (P1), as illustrated in the structural model (see Figure 1.1).
- **Question Two.** *To what extent does information security awareness influence a Facebook user's intention to use Facebook Apps?* The aim of this question was to evaluate the second proposition (P2), as illustrated in the structural model (see Figure 1.1).
- **Question Three.** *To what extent does social norms influence a Facebook user's intention to use Facebook Apps?* The aim of this question was to evaluate the third proposition (P3), as illustrated in the structural model (see Figure 1.1).
- **Question Four.** *To what extent does a Facebook user's personality traits influence their behaviour towards the intended use of Facebook Apps?* The aim of this question was to evaluate the fourth proposition (P4), which is illustrated as the dotted rectangle surrounding the five personality traits that form part of the Big Five (see Figure 1.1).

1.4 Research objective

The objective of this study was to develop a personality-based surveillance model for Facebook App users. This model was subsequently used to evaluate the influence of a Facebook user's personality traits, attitude, social norms and information security awareness (used as a behavioural control) on their intent to make use of Facebook Apps. Within the context of this study Facebook Apps acts as one of the mechanisms used to perform surveillance of Facebook-based personal information. Although previous studies in this field made use of personality traits - specifically the Big Five - they had a different focus, ranging from the analysis of Facebook profile content (Ortigosa et al., 2014), qualitative assessments based on observations (Qiu et al., 2012), to artificial intelligence processing (Lima & De Castro, 2014).

Studies with similar objectives either focused on information privacy (Castañeda et al., 2007; Chellappa & Pavlou, 2002), Facebook's privacy settings within an advertising context (Heyman et al., 2014), the usage of Facebook (Ryan & Xenos, 2011) or simply qualitative analyses, based on surveillance theory (Marwick, 2012). Additionally, although there are studies that explore the information privacy concerns of social media users, these studies neglect to relate this to personality traits (Krasnova et al., 2009). Those studies that do evaluate the influence of personality traits do not focus on Facebook Apps. As such, few (if any) have developed models to explore the extent to which personality traits influence a social media user's intention to make use of Facebook Apps given the additional behavioural influence of attitude, social norms and information security awareness.

1.5 Methodological approach

This study was conducted within the post-positivist paradigm because it adapted an existing theoretical model (i.e., the Theory of Planned Behaviour). Additionally, since propositions were developed instead of hypotheses, an inductive approach to theory development was adopted, culminating in the development of a conceptual research model. To support the development of the propositions, secondary data was collected via a scoping literature review and analysed by way of a content analysis that spanned three phases.

This study also collected primary data by adopting a survey methodology. As such, a large-scale survey was conducted by making use of Amazon Mechanical Turk (AMT). To qualify for this survey respondents had to fulfil the following criteria:

- They had to be citizens of the United States of America (USA),
- They had to be at least 18 years of age, and
- They had to be active Facebook users.

After initial pilot testing, the final questionnaire was used to collect primary data. This questionnaire consisted of 96 items and where possible the items were either directly taken from other sources or adapted accordingly (see Appendix A for a complete list of these items). The bulk of these are associated with the constructs of the research model and are distributed as follows:

- The construct *Intention to use Facebook Apps* (one item),
- The construct *Attitude towards privacy* (seven items),
- The construct *Social norms* (seven items),
- The construct *Information security awareness* (twelve items), and
- The five personality traits namely, *Openness to Experience*, *Agreeableness*, *Extraversion*, *Neuroticism* and *Conscientiousness* (illustrated as constructs on the far left of Figure 1.1) were evaluated by forty-four items, as prescribed by the Big Five Inventory (BFI) (John & Srivastava, 1999).

Additionally, the questionnaire also contained items that captured information relating to:

- Respondent demographics (three items),
- Social desirability (eight items),
- Attention traps (two items),
- Facebook and PC experience (three items), and
- Facebook usage (ten items).

Since the exact number of US citizens who are registered on AMT is unknown, and this number is likely to fluctuate, non-probability sampling was used. Using the questionnaire, a total of 651 responses were collected, of which 537 were deemed usable.

After the data was collected, validity and reliability testing was conducted, resulting in the elimination of several items due to low factor loadings (see Appendix A). Using a deductive approach the propositions were statistically evaluated by employing a multivariate analysis technique referred to as Partial Least Squares (PLS) path modelling.

Given the number and the complexity of the relationships illustrated in the research model, SEM is an appropriate multivariate technique (Gefen et al., 2000). This stems mainly from the fact that it allows for the estimation of multiple path coefficients (the relationships between constructs) simultaneously. In other words, only one structural model needs to be developed to evaluate the propositions.

Table 1.1: Summary of the personality trait's level of vulnerability

	Openness to Experience	**Conscientiousness**	**Extraversion**	**Agreeableness**	**Neuroticism**
Core characteristics	*Non-conformist, intellectual and inquisitive.*	*Emotionally stable, goal-oriented and not easily influenced.*	*Sociable, easily influenced and open to risky behaviour.*	*Self-conscious, easily influenced and trusting.*	*Emotionally unstable, distrustful and negative.*
Vulnerability	*Positive relationship with information security awareness (**Thus, less vulnerable**).*	*Positive relationship with information security awareness. Positive attitude towards privacy (**Least vulnerable**).*	*Susceptible to influence of norms and exhibits negative attitude towards privacy (**Most vulnerable**).*	*Susceptible to influence of norms and exhibits a positive attitude towards privacy (**More vulnerable; especially if influenced by peers**).*	*Positive relationship with information security awareness (**Thus, less vulnerable**).*
Vulnerability level	**2**	**1**	**5**	**4**	**3**

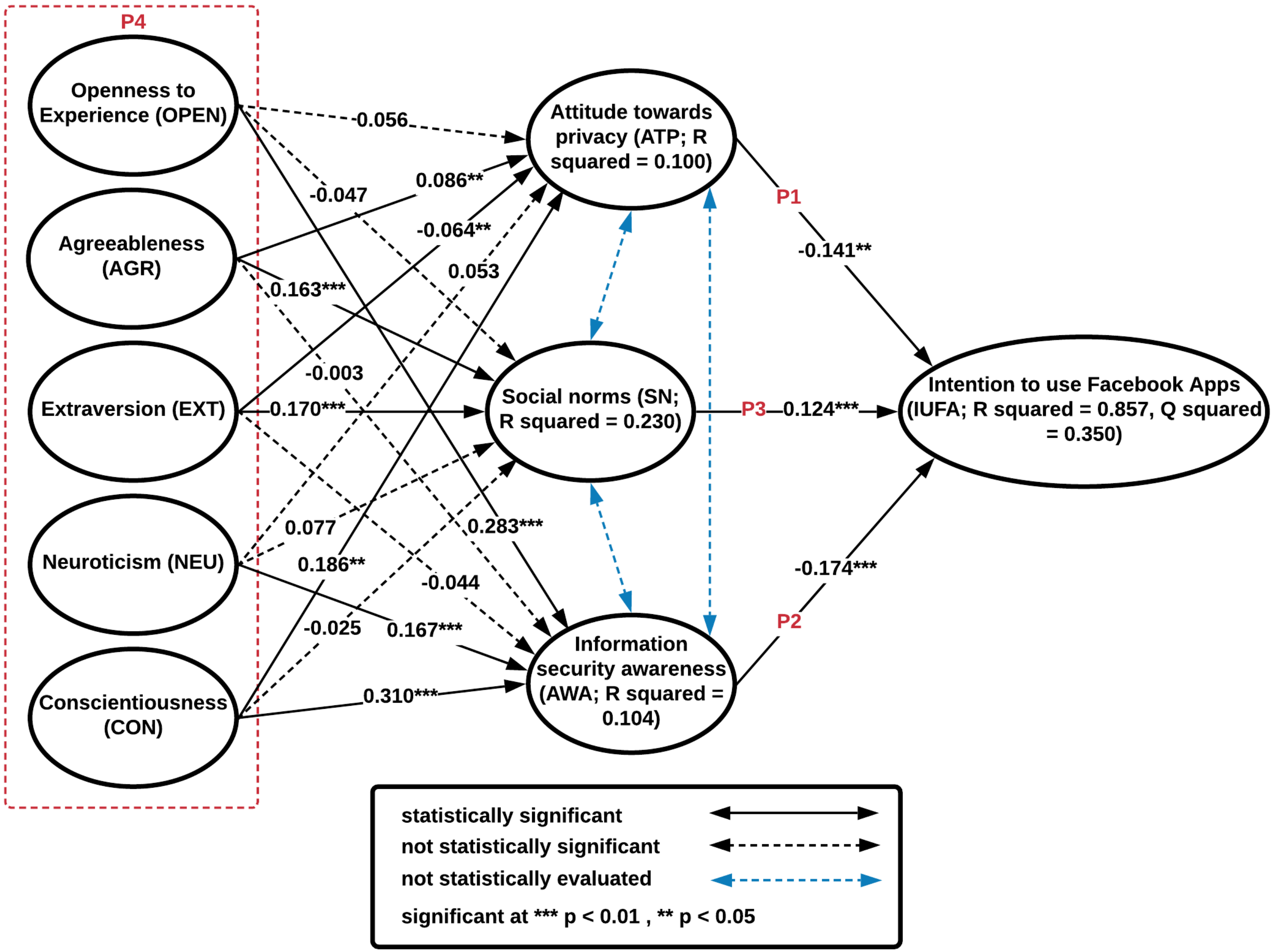

P4
Openness to Experience (OPEN)
Agreeableness (AGR)
Extraversion (EXT)
Neuroticism (NEU)
Conscientiousness (CON)
Attitude towards privacy (ATP; R squared = 0.100)
Social norms (SN; R squared = 0.230)
Information security awareness (AWA; R squared = 0.104)
Intention to use Facebook Apps (IUFA; R squared = 0.857, Q squared = 0.350)
-0.056
-0.047
0.086**
-0.064**
0.053
0.163***
-0.003
0.170***
0.077
0.283***
0.186**
-0.044
-0.025
0.167***
0.310***
P1
-0.141**
P3
-0.124***
P2
-0.174***
statistically significant
not statistically significant
not statistically evaluated
significant at *** p < 0.01 , ** p < 0.05

Figure 1.1: Personality-based Facebook App surveillance model

1.6 Contribution

This study contributes to known theory within the field of behavioural information security by indicating the level of vulnerability based on an individual's personality traits. The levels of vulnerability were determined by interpreting both the structural model (see Figure 1.1) and known personality theory. For example, individuals high in Extraversion were found to be particularly vulnerable followed by individuals high in Agreeableness (see Table 1.1).

As stated, few (if any) previous studies have been found to be similar, with several studies alluding that this is still a relevant and persistent problem which requires further research (Benson et al., 2015; Karwatzki et al., 2017; Saridakis et al., 2016; Wilson et al., 2010). Moreover, the inclusion of *Social norms*, which incorporates both descriptive and subjective norms, also contribute to known theory in this context. For example, norm-based studies of Apps (whether mobile, social media or specifically Facebook-based) have only been studied by focusing on either subjective norms or descriptive norms (Pu & Grossklags, 2015), but not both. Additionally, those studies that have investigated other behavioural aspects of Apps (Farnden et al., 2015; Golbeck & Mauriello, 2016) have not included any norms as part of their research models. This study also incorporated information security awareness instead of Perceived Behavioural Control as a means to argue the behavioural influence of both awareness and knowledge acquisition.

1.7 Ethical considerations

From an ethical point of view, research conducted on social media platforms should be subjected to specific ethical considerations. This stems from the potential to cause harm to a large number of individuals (Kosinski et al., 2015). The lack of formal, and often contradictory guidelines complicates matters even further. According to the British Psychological Society (2007), Internet Mediated Research (IMR) should be viewed in the same light as traditional human-based research, with the understanding that there are additional ethical concerns to consider.

Foremost amongst these is the need to inform social media users about one's intentions to use their information. Given the psychological nature of the study, the ethical clearance application included the endorsement of a psychometrist who was used to oversee the scoring of the responses related to the forty-four items used, to determine an individual's personality traits. Together, these documents were submitted to the Rhodes University central ethics committee, which subsequently granted full ethical clearance (clearance ID: CIS18-10).

1.8 Thesis outline

In this study, Chapter 2 provides the reader with a complete overview as to the research design and methodology. This includes a detailed discussion as to the sources of secondary and primary data, as well as how these sources were analysed. Chapter 3 provides a detailed review of the literature pertaining to the surveillance of data. It not only provides historical evidence of such activities, but also indicates how such practices have evolved and subsequently been adopted by social media corporates, like Facebook. This is followed by Chapters 4 and 5, which provide a detailed overview of the literature as it relates to the behavioural influence of personality, attitude, awareness, and social norms. Together, Chapters 3, 4 and 5 provide the necessary support for the propositions of this study. Chapter 6 provides some additional support for each of the four propositions. It also formally states the four propositions concluding with an illustration of this study's conceptual research model. This is followed by Chapter 7, which presents the results of this study's univariate and multivariate analyses. Importantly, Chapter 7 also formally illustrates the Personality-based Facebook App surveillance model (Figure 1.1) providing evidence that the model is structurally sound. Chapter 8 provides readers with a detailed discussion based on the interpretation of the results illustrated by the structural model. This discussion is specifically aligned with both the propositions and their associated research questions. Chapter 9 provides a retrospective overview of the entire thesis in the form of a conclusion, with a specific focus on how the research questions of the study have been answered.

Chapter 2

RESEARCH DESIGN AND METHODOLOGY

> "I think one's feelings waste themselves in words; they ought all to be distilled into actions which bring results."
>
> — Florence Nightingale

This chapter discusses the various components that constitute the research design and methodology of this study. To this end, the discussions will elaborate on the philosophical assumptions, the research, the data collection methods, and the sources of data, as well as the analysis thereof, within the context of both the pilot and the final study. Note that a detailed account of the process of analysis for secondary data is provided in this chapter, so as to convey this process as a whole, rather than providing only the diagrams and the research results in Chapter 7, out of context.

2.1 Design overview

After a research problem has been defined Kothari (2004, p.14) suggests creating a conceptual design of the research to follow (see Figure 2.1).

This not only aids conducting the research as efficiently as possible but also ensures that the maximum amount of relevant data is collected as dictated by the purpose of the study.

In line with these, two research designs are outlined by Kothari (2004, p.14) as illustrated in Table 2.1. From this, it is possible to deduce that this study is descriptive in nature since:

- It employs a rigid cross-sectional design (Giles, 2013, p.100) where the sample was only evaluated once (overall structured approach as outlined in this chapter),
- United States Facebook users were surveyed using a predetermined sampling strategy,
- The statistical methods of analysis were planned upfront, based on set criteria,
- A structured survey was used to collect primary data, and
- The study has clear operational plans guided by the evaluation of the propositions within the confines of the research model.

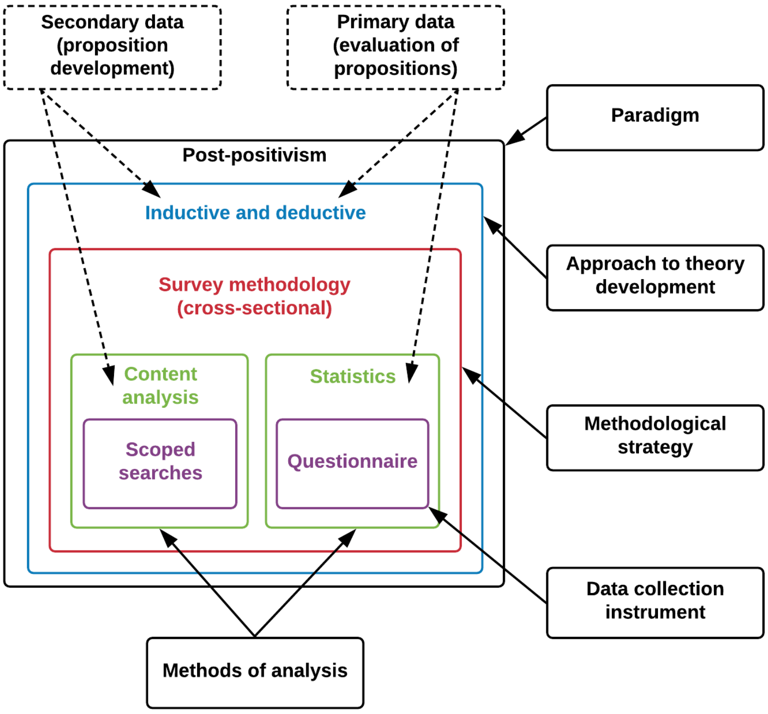

Secondary data (proposition development)
Primary data (evaluation of propositions)
Paradigm
Post-positivism
Inductive and deductive
Approach to theory development
Survey methodology (cross-sectional)
Content analysis
Statistics
Methodological strategy
Scoped searches
Questionnaire
Data collection instrument
Methods of analysis

Figure 2.1: Illustration of this study's research design

Social research, in particular, makes use of such descriptive research designs, which closely aligns with this study's focus on Facebook user perceptions and their resultant behavioural influences.

Table 2.1: Comparison of research designs

Design aspects	Exploratory	Descriptive/Diagnostic
Overall	Flexible design	Rigid design
Statistical Analysis	Analysis is not planned	Analysis is planned
Observation	Unstructured data collection instruments	Structured data collection instruments
Operational	No operational plans	Extensive operational plans

2.2 Philosophical perspective

According to Burns (2000), research can be described as a method of systematically investigating phenomena which typically involves data collection, analysis and interpretation, as part of a larger research design. As the first step towards defining such a research design Mackenzie & Knipe (2006) suggest choosing a research paradigm. This serves the following purposes:

- It outlines the intention of the research to be undertaken,
- It provides a clear indication of underlying motives and further methodological choices, and
- It allows other researchers to understand what to expect in terms of the type of results and findings to be made.

Often referred to as the theoretical framework (distinct from theory), the choice of paradigm ultimately allows researchers to question their worldviews. Such worldviews not only influence how data is collected but also which data was deemed important to collect. For the most part, these are philosophical questions, differing greatly from one researcher to the next, even though the research is in related fields. For example, a single research project may require the input of various research groups that each investigate a small portion of the larger problem. Software engineers are likely to employ engineering techniques to build and to test software, whereas researchers within the field of user experience are likely to use surveys, interviews, and prototyping as part of their methodological approach. Both groups are involved in solving the larger problem - albeit using different methods. Different research groups are also likely to have diverse views as to what constitutes not only knowledge, but also the construction thereof. The same applies to their views on reality and those processes that shape it. Collectively these different views regarding knowledge and reality are referred to as philosophical assumptions with each paradigm's assumptions, taking on a different form.

2.2.1 Positivist and post-positivist paradigm

The term positivism was first used by the French philosopher Auguste Comte (circa 1798) who argued that knowledge has to pass through three stages: theological, metaphysical and finally the positivist state. For these theorists knowledge only became useful when it reached a positivist state - hence the word positivism (Miller, 2000). Positivism purports that a complete understanding of phenomena can be obtained by methodologies that employ experimentation and observation (Miller, 2000) - commonly referred to as the scientific method (Ryan, 2006). For positivists, formal theory and the collection of empirical data is seen as the most important aspect regarding knowledge creation. For this reason, human perspectives are abstracted and presented as that which is universal and acontextual. Ontologically, positivism engenders beliefs of a reality that exists outside the social experiences of daily life. Epistemologically, positivism seeks to replicate and generalise by testing theories (Mackenzie & Knipe, 2006). As such, knowledge claims should be able to stand up to verification as well as to falsification. For this reason, positivist researchers typically use quantitative research instruments, such as questionnaires. In fact, positivists generally (Mackenzie & Knipe, 2006):

- Formulate hypotheses, which are evaluated using construct-based models,
- Usually employ quantitative methods, such as questionnaires to test the models, and
- Take a value-free stance on research matters.

Similarly, post-positivists also endeavour to test and evaluate theories. However, they do so with the assumption that their own and any other form of research is directly influenced by an already established theoretical framework (Hamati-Ataya, 2012). Ontologically, post-positivists concede that individuals, cultures, and social groups function within the context of multiple realities. They accept that there is no absolute truth and that what is perceived as accurate for one individual or group is not universally applicable to other members of the same or other groups (Miller, 2000). According to O'Leary (2004, pp.6-7) post-positivism is exploratory, making use of inductive reasoning to generate findings that are often qualitative. Notwithstanding the differences, post-positivists also make use of quantitative data collection instruments.

2.2.2 Interpretivist paradigm

Unlike positivists, who view reality as objective truth, interpretivism strives to understand the world and reality as experienced by those individuals who participate therein (Mackenzie & Knipe, 2006). As such, ontologically interpretivism assumes that reality is socially constructed. Additionally, the life experience and background of the researcher is assumed to impact on research undertaken within this paradigm. Unlike post-positivist research, interpretivism does not start the research process with a predetermined theory, but rather develops it as the research unfolds. Both qualitative and quantitative research methods (mixed methods) apply to this paradigm.

2.2.3 Pragmatist paradigm

Usually employed as a means to answer both *what* and *how* questions, pragmatism rejects the idea of a single objective reality. Often used as the underlying philosophical perspective of mixed methods research, the problem statement is given the utmost importance, and all manner of methods are applied to solving it. As such, a wide variety of data collection and analysis methods are usually employed, making it the least aligned paradigm from a philosophical perspective (Mackenzie & Knipe, 2006).

2.2.4 Transformative paradigm

One methodology commonly used as part of the transformative paradigm is critical theory. Critical theory's core assumption is to improve society at large (Ngwenyama, 1991). Stahl (2008) rephrases this stating that critical researchers wish to support and bring about change. As such, the most essential aspect of critical research is the notion of improving a given social situation by consulting history to understand why societal changes have not taken place (Stahl, 2006). For Walsham (2005), critical research has a personal connotation fixated on all that is wrong with the world. Humans are viewed as an object instrumental in the process that leads to the formation of a problem, as well as the perceptions that shape the answers.

Unlike traditionalists (such as positivist researchers) critical theorists seek not to uphold the status quo, but rather to investigate existing social phenomena to emancipate man (Myers & Klein, 2011; Ngwenyama, 1991). Orlikowski & Baroudi (1991) refers to critical research as an evaluative approach whereby researchers attempt to transform specifically the socially constructed reality of the subjects under investigation. Its main concern is the excavation of societal contradictions. Stahl, expands on this definition, stating that critical research endeavours to,

> *"...overcome injustice and alienation..." (Stahl, 2008, p.139).*

Formally, there are several assumptions upon which critical social theory is based. Firstly, people are the creators of their social world. Secondly, and unlike positivism, all scientific knowledge is socially constructed and value-laden. Thirdly, reasoning, and critical inquiry should function in unison, ensuring that theory and practice are not separated. Lastly, critical theorists should not use it in isolation from the social phenomena it sets out to change (Ngwenyama, 1991).

2.2.5 The paradigm used in this study

This study assumes that Facebook users experience multiple realities and that unlike in pure positivist-based research, there is no ultimate and purely objective truth or reality. Given that Facebook and social media, in general, facilitate the creation of many shapes and forms of what other users deem reality, this makes for a logical choice (Mackenzie & Knipe, 2006). Ontologically, Facebook users do create their realities via social interaction, but these may be based on varied beliefs - some of which are flawed. For example, some users may believe that Facebook does not misuse their personal information based on their sentiment towards Facebook Apps. According to Miller (2000) post-positivism *tempers* such beliefs in that they may not fully understand their assumed realities - especially the mechanisms that influence them.

In this study, awareness of Facebook App surveillance acts as one such *temper* mechanism, since although users experience their own constructed reality, they may not comprehend what drives the resultant behaviour; not their behaviour as such, but rather the surveillance-related behaviour of Facebook. As such, post-positivism enables this study to investigate users' constructed realities, as influenced by their perceptions and resultant judgement thereof. The ontological correctness of these perceptions and their associated beliefs are not of concern in this study - only the user's intended behaviour as a result of these beliefs. For example, some respondents may believe that awareness is not essential to Facebook App surveillance or that social norms do not influence their resultant intentions. These beliefs are essential and are not rejected in favour of beliefs based on a single objective truth. This study does not enforce the belief that all the constructs are equally important, irrespective of the beliefs captured by the data collection instrument. Instead, each respondent's beliefs are captured, forming part of a larger dataset comprising many beliefs, based on different realities. The latter thus implies that the resultant dataset takes on a patterned and somewhat predictable form since it is accepted that at least some of the respondents' beliefs overlap in some way - a trademark of post-positivist research (Miller, 2000).

2.3 Approach to theory development

As outlined by Saunders et al. (2016, p.166), a research design can use abductive, inductive, or deductive reasoning to develop theory. Note that these approaches are not necessarily mutually exclusive. For example, in this study, both inductive and deductive reasoning was used - albeit within different phases of the research design. Firstly, inductive reasoning was used during the process of analysing the secondary data. This enabled the development of the research model and associated propositions. After this, deductive reasoning was used to evaluate this study's propositions using the statistical methods outlined in this chapter.

2.4 Methodological strategy of this study

Adapting the discussions of Mertens (2014), Mackenzie & Knipe (2006) illustrates several methodological approaches, where methodologies are viewed as named collections of methods that inform how the research is to be conducted. For (Kothari, 2004, p.8) a methodology is primarily,

> *"...a way to systematically solve the research problem."*

Methods and techniques need to be motivated, considering the criteria for their use. Kothari (2004, p.8) uses the example of an architect who has to decide on what criteria his use of doors, windows, and building structures are based. In this example, the doors and the windows can be seen as research methods, since they are generic enough to fit into many different applications of the same research methodology.

In general, researchers can choose from several methodologies including, survey, case study, action research, grounded theory, ethnography, or even archival research (Saunders et al., 2016). This study adopted a non-experimental (i.e., data was not manipulated during evaluation) (Punch, 2003) survey methodology for both the primary and the secondary data, since either an a-priori theory (the Theory of Planned Behaviour) or a coding framework (for secondary data) was used. This ensured that the methodology aligned with the study's choice in paradigm (i.e., post-positivism).

2.5 Secondary data collection in this study

Secondary data (literature) was collected in a systematic manner by way of several scoping reviews so as not to strictly limit relevant literature (Peters et al., 2015). It is from these scoping reviews that the four propositions, research model, and associated research instrument was created.

2.5.1 Sources of secondary data

The source of secondary data comprised several academic databases in additional to relevant gray material (i.e, web articles, white papers and guides). Secondary data sources were consulted to substantiate and further develop the research problem but also to ascertain how surveillance practices have evolved. In other words, initial literature searches were specifically geared to provide clarity as to how the surveillance of data took place before the advent of social media.

As such, to adequately argue the historical context and the persistence of data surveillance, it was decided that the required literature searches were to be done going back as far as 1970. These initial search phases included not only keywords related to the study's problem statement, but also those that featured within articles written by authors who focus on the surveillance of data in that era. For example, authors such as Clarke (1988) and Lyon (1992) make extensive reference to the surveillance of data by referring to it as *computer matching* or *dataveillance*. As such, these terms were primarily used in the initial literature searches, which led to the identification of several articles from a number of academic databases, as illustrated in Table 2.2.

Table 2.2: Sources of secondary data to argue the historical context - phase one

Academic databases	**Number of articles**
ACM	1
JSTOR	132
ScienceDirect	106
Sage	20
Taylor Francis	15
Springer Link	225
AIS Senior Scholars Journals	3

At this point, all of the identified articles were subjected to an initial screening process. This entailed reading each article's title and abstract to ascertain relevance within the context of the larger argument to be made. Initial screening also checked for duplication among the articles. Each article was also read in its entirety to ensure that the content was related to the historical context of the research problem. This process is visually illustrated in Figure 2.2 as a Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) diagram, which also contains the numerical values that comprised this process of secondary data collection.

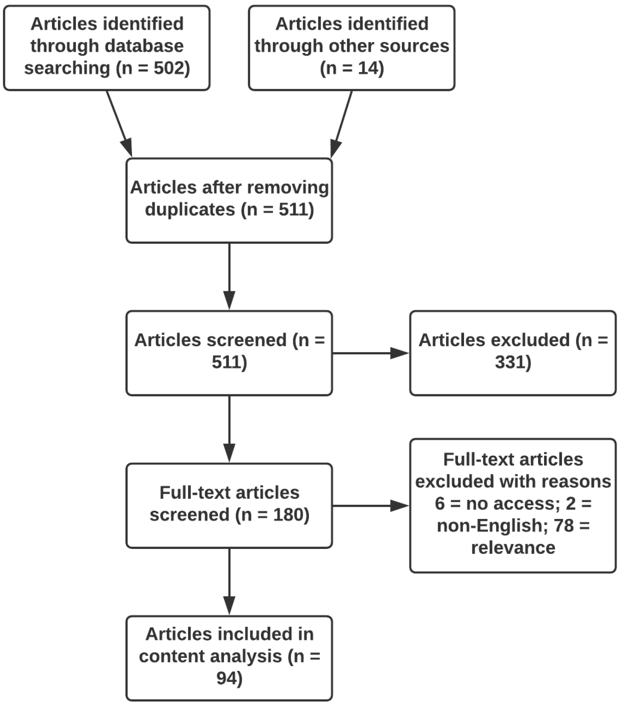

Articles identified through database searching (n = 502)
Articles identified through other sources (n = 14)
Articles after removing duplicates (n = 511)
Articles screened (n = 511)
Articles excluded (n = 331)
Full-text articles screened (n = 180)
Full-text articles excluded with reasons 6 = no access; 2 = non-English; 78 = relevance
Articles included in content analysis (n = 94)

Figure 2.2: PRISMA of search phase one

Because the historical context forms only one part of the problem chapter (Chapter 3), additional secondary data had to be collected to argue how this applies to social media in general and to Facebook in particular. The same process of data collection took place as outlined above with the exception that the search phrases had to be adapted since the interest was now on how (and why) social media corporates (like Facebook) perform the surveillance of data.

As before, articles written by prominent authors on the topic of social media surveillance were used as an indication as to what keywords to use in subsequent searches. For example, from Fuchs (2011), it is clear that social media corporates conduct surveillance for economic reasons - hence the addition of the search phrases *economic surveillance* and *social media surveillance*. This was followed by a series of literature searches on a similar set of academic databases as before. However, in this second search phase, it was decided that only articles published in or after 2004 would be included since this was the year Facebook launched. The results of this search process are illustrated in Table 2.3.

After removing duplicates, the same screening processes were conducted. Unlike the first search phase, additional articles and books were identified when backward searching was conducted using the references sections of critical articles. For example, the book *Social Media: A Critical Introduction* (Fuchs, 2017) was instrumental in understanding how the

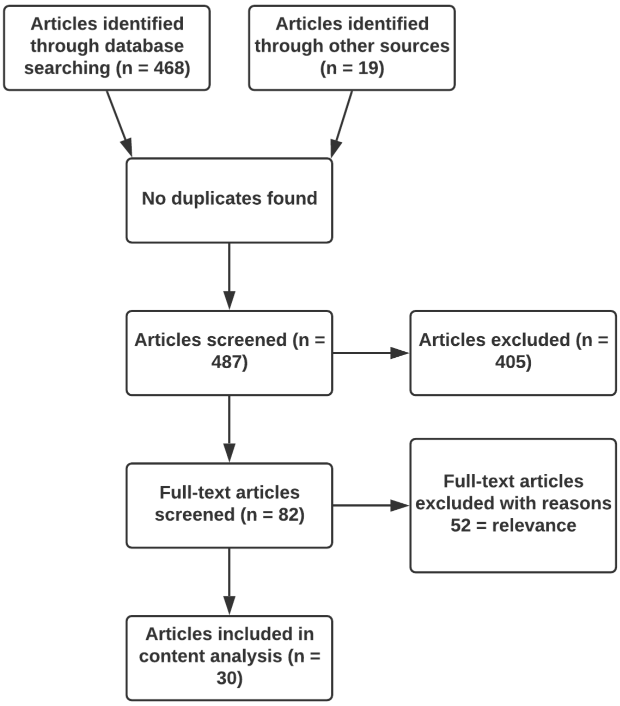

Articles identified through database searching (n = 468)
Articles identified through other sources (n = 19)
No duplicates found
Articles screened (n = 487)
Articles excluded (n = 405)
Full-text articles screened (n = 82)
Full-text articles excluded with reasons 52 = relevance
Articles included in content analysis (n = 30)

Figure 2.3: PRISMA of search phase two

Table 2.3: Sources of secondary data to argue social media surveillance - phase two

Academic databases	Number of articles
ACM	3
IEEE	4
JSTOR	46
ScienceDirect	180
SCOPUS	7
Sage	29
Taylor Francis	54
Springer Link	133
AIS Senior Scholars Journals	12

surveillance problems within the review of the historical context evolved and influenced the creation and the surveillance conducted within social media. Importantly, no gray literature was identified in these early search phases. The final set of articles used for the second search phase is illustrated by the PRISMA diagram in Figure 2.3.

Together, the data sources identified in the first and second search phases enabled the development of Chapter 3 and parts of Chapter 1. The development of Chapter 4 and 5 required the collection of additional secondary data since it became apparent that much of the surveillance conducted by social media corporates are fundamentally driven by an individual's need to communicate. The more such communication takes place on a social media platform, the more personal information there is to perform surveillance on (i.e., harvest). Further reading on the matter - specifically the work of Martinez (2017) - led to a realisation that in no small degree, most individual's participation in social media is behaviour driven. However, to adequately argue and substantiate this, additional secondary data had to be collected as part of a third search phase.

Using the same approach as before, the third search phase used phrases to find secondary data on behaviour and those psychological factors that influence it. This entailed conducting literature searches using phrases such as *behavioural influence* and *social media use*. In this instance, the number of results was too large to effectively screen, requiring a more focused search strategy. To this end, a number of psychological factors, such as self-esteem, loneliness, and need for closure (among others) were identified. Since Facebook alone attracts over 2 billion users daily, it was thought unlikely that social media corporates would hinge their platform's appeal on such specific psychological factors. What did make sense was to find a behavioural aspect that every human possesses, namely, personality. Subsequent searches were guided by including *personality*. These search results were not only more focused, but also enabled the creation of specific research questions by including keywords such as *social norms*, *attitude*, *information security awareness*, *behaviour* and *personality*. This resulted in the identification of journals from a variety of databases, as illustrated in Table 2.4.

This was followed by the two screening processes as well as a check for duplicate articles. It is worth noting that additional backward searching was required during the second screening phase since:

Table 2.4: Sources of secondary data - phase three

Academic databases	Number of articles
IEEE	2
JSTOR	45
ScienceDirect	88
SCOPUS	2
Sage	68
Taylor Francis	11
Emerald Insight	17
AIS Senior Scholars Journals	15

- A large proportion of the personality theory was located in books instead of journals.
- Several relevant articles were identified that illustrated the behavioural influence of attitude, social norms, and awareness, but were not necessarily information security based.
- It allowed for the identification of several theoretical models to consider adapting for this study. These included, Privacy Calculus, Theory of Reasoned Action, Protection Motivation Theory, Uses and Gratification Theory as well as the Theory of Planned Behaviour, and
- Additional relevant concepts relating to Facebook App surveillance was identified. These included information privacy, institutional trust, as well as the need to provide a detailed breakdown of social norms. For example, several articles consistently used subjective, descriptive and injunctive norms.

See Figure 2.4 for the PRISMA diagram that accompanied the third search phase.

2.6 Process of secondary data analysis

Both the primary and the secondary data underwent structured forms of analysis. In the case of the secondary data, an inductive approach was adopted, leading to the development of this study's research model constructs, relationships, and propositions. The process of analysing the secondary data took place over three phases. Here the final set of articles identified through each of the three search phases was imported into a Qualitative Data

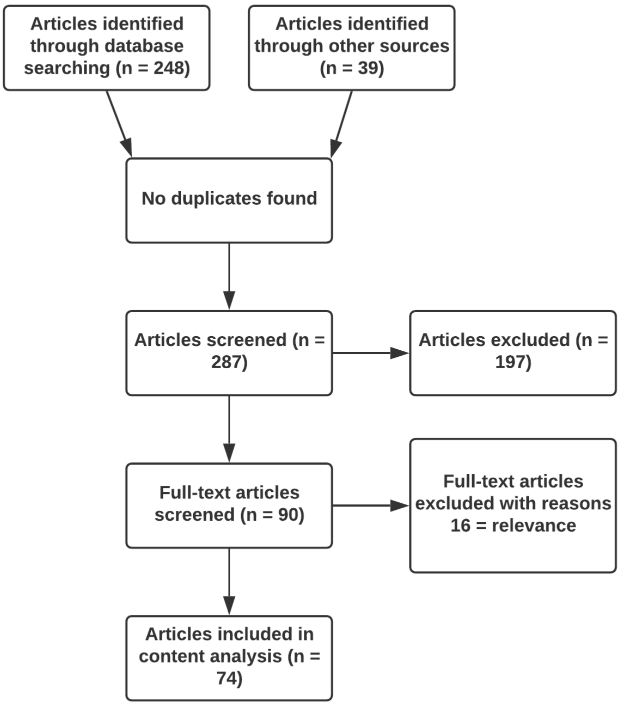

Articles identified through database searching (n = 248)
Articles identified through other sources (n = 39)
No duplicates found
Articles screened (n = 287)
Articles excluded (n = 197)
Full-text articles screened (n = 90)
Full-text articles excluded with reasons 16 = relevance
Articles included in content analysis (n = 74)

Figure 2.4: PRISMA of search phase three

Analysis Software (QDAS) package called Atlas.ti. 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). Such analyses not only lead to the identification of latent themes but also areas of theoretical overlap.

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 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) suggests that researchers create an a priori coding framework before engaging with the software making this an ideal method of data analysis within the adopted post-positivist paradigm. The resultant analysis spanned three phases with the coding framework forming a core component within the first phase. Although the second and third phases of the content analysis still made use of the initial framework, its primary focus was on coding for relevant content in an inductive manner. As such, specific codes were merged into what Atlas.ti calls code groups. In turn, this provides support for this study's propositions.

2.6.1 First phase of analysis

In the first phase of analysis, the 94 articles relating to the surveillance of data were analysed. All the articles were inductively coded based on the initial scoping reviews' search phrases. As such, any content related to dataveillance and surveillance was first quantified (209 codes representing 2535 quotations) and then merged into appropriate code groups (8 groups). Code groups such as those listed below were created by merging related codes after a process of visually inspecting their related network diagrams (see Figure 2.5 for an example network).

- *surveillance:enablers*,
- *surveillance:decentralised concept*, and
- *surveillance:link to prosumption*.

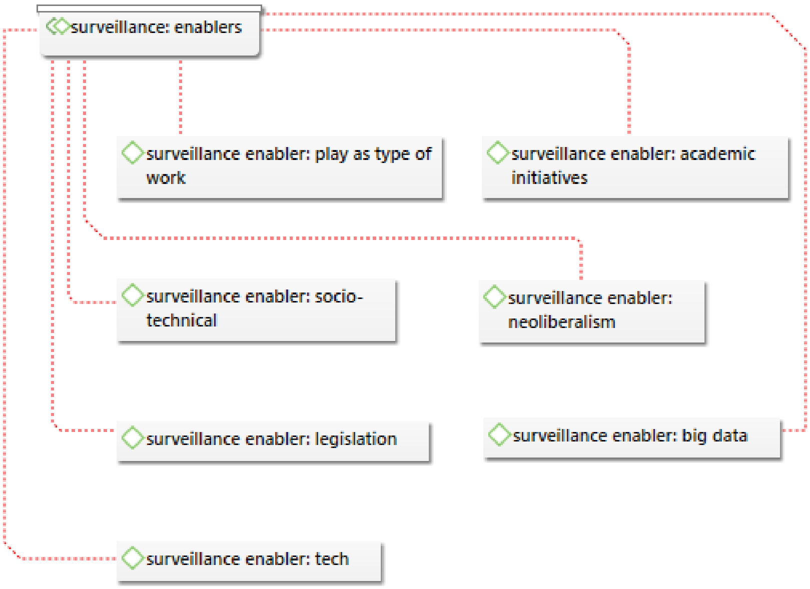

surveillance: enablers
surveillance enabler: play as type of work
surveillance enabler: academic initiatives
surveillance enabler: socio-technical
surveillance enabler: neoliberalism
surveillance enabler: legislation
surveillance enabler: big data
surveillance enabler: tech

Figure 2.5: Atlas.ti network of a first phase code group

Once merged, the resultant code groups became the foundation of the content in Chapter 3. For example, the quotes associated with the code group *surveillance:enablers* were used to write parts of Section 3.1.3.

Because the majority of these articles were analysed within the context of this study's problem, the research model constructs were not derived from this narrative.

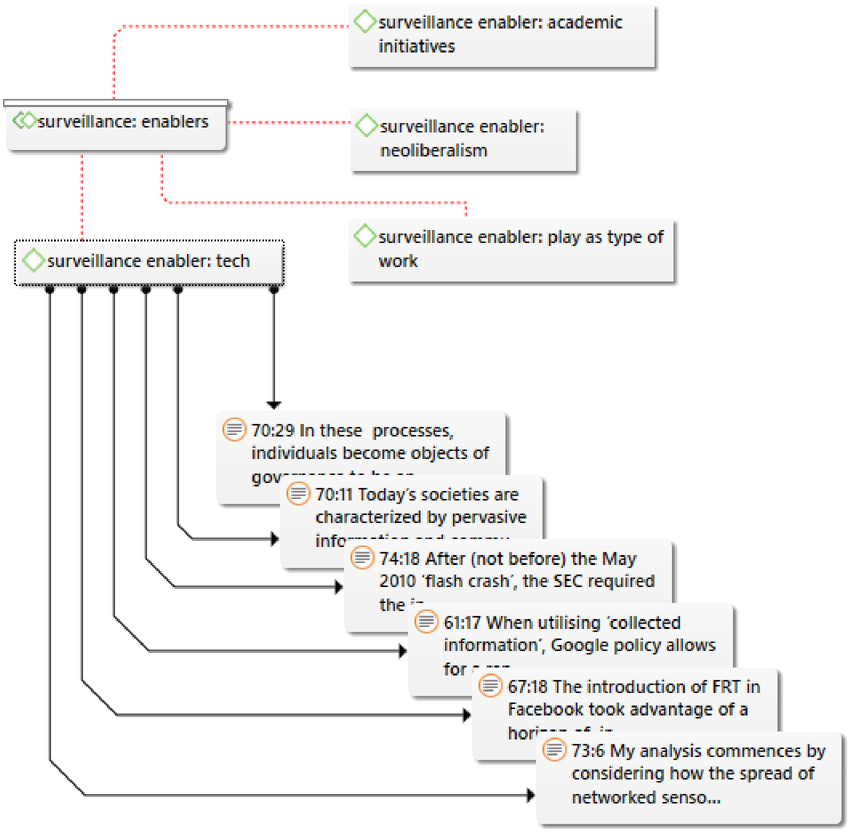

surveillance enabler: academic initiatives
surveillance: enablers
surveillance enabler: neoliberalism
surveillance enabler: play as type of work
surveillance enabler: tech
70:29 In these processes, individuals become objects of gov...
70:11 Today's societies are characterized by pervasive info...
74:18 After (not before) the May 2010 'flash crash', the SEC required the i...
61:17 When utilising 'collected information', Google policy allows for a...
67:18 The introduction of FRT in Facebook took advantage of a horizon of in...
73:6 My analysis commences by considering how the spread of networked senso...

Figure 2.6: Example of Atlas.ti quotes

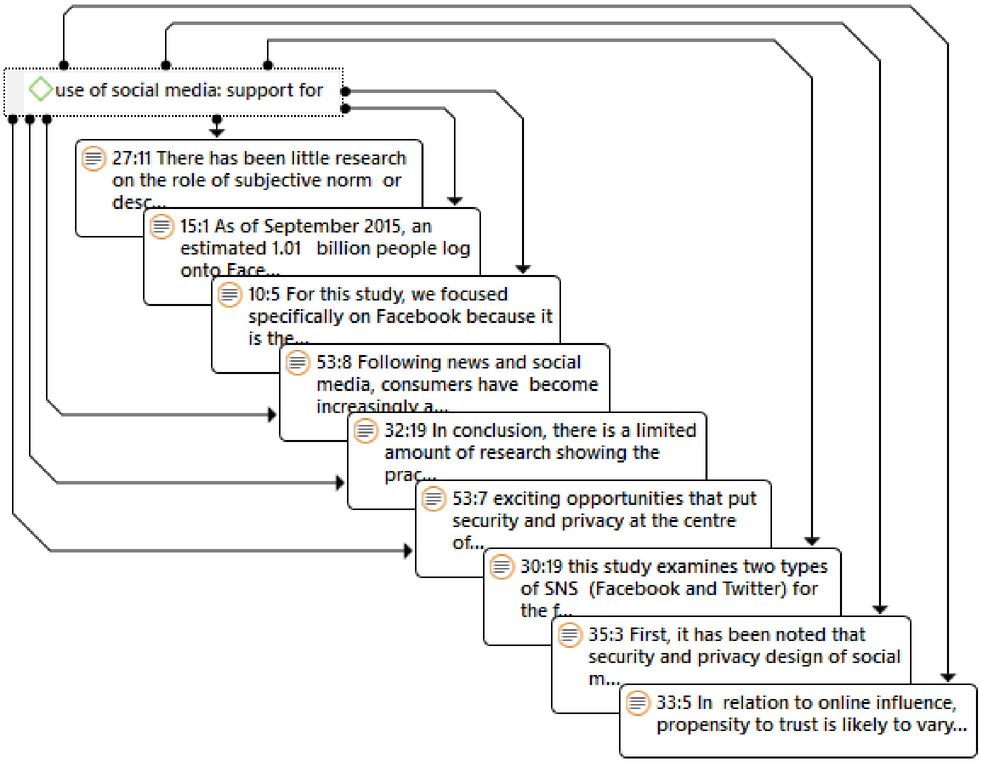
2.6.2 Second phase of analysis

The purpose of the second phase of analysis was to argue the surveillance of data as it relates to social media. In turn, this entailed a more in-depth analysis due to this study's focus on social media. In this regard, 17 codes (associated with 105 quotations) were created and eventually merged into 10 code groups. Atlas.ti codes such as, use of *social media:support for* and *social media:background* were instrumental in linking the behavioural aspects of this study to social media (see Figure 2.7 and 2.8 for related networks).

Similar to the first phase, none of the resultant narratives assisted the theoretical development of this study's propositions.

2.6.3 Third phase of analysis

Several of the behavioural studies analysed in phase two confirmed the relevance of a personality-based approach in this study. Comprising 443 quotations, 58 codes, and 16 code groups this phase of analysis required an in-depth understanding as to how an individual's personality influences their behaviour. Doing so also highlighted the usefulness of



use of social media: support for

27:11 There has been little research on the role of subjective norm or desc...

15:1 As of September 2015, an estimated 1.01 billion people log onto Face...

10:5 For this study, we focused specifically on Facebook because it is the...

53:8 Following news and social media, consumers have become increasingly a...

32:19 In conclusion, there is a limited amount of research showing the prac...

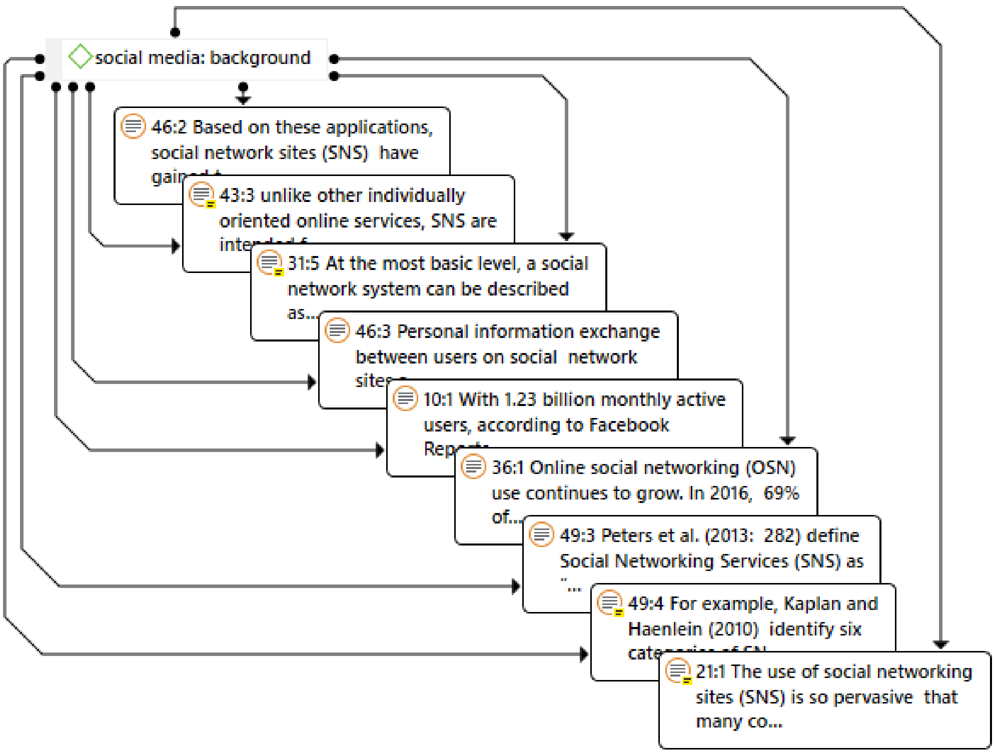
53:7 exciting opportunities that put security and privacy at the centre of...

30:19 this study examines two types of SNS (Facebook and Twitter) for the f...

35:3 First, it has been noted that security and privacy design of social m...

33:5 In relation to online influence, propensity to trust is likely to vary...

Figure 2.7: Atlas.ti code linking behaviour with the use of social media



social media: background

46:2 Based on these applications, social network sites (SNS) have gained t...

43:3 unlike other individually oriented online services, SNS are intended f...

31:5 At the most basic level, a social network system can be described as...

46:3 Personal information exchange between users on social network sites...

10:1 With 1.23 billion monthly active users, according to Facebook Reports...

36:1 Online social networking (OSN) use continues to grow. In 2016, 69% of...

49:3 Peters et al. (2013: 282) define Social Networking Services (SNS) as "...

49:4 For example, Kaplan and Haenlein (2010) identify six categories of SN...

21:1 The use of social networking sites (SNS) is so pervasive that many co...

Figure 2.8: Atlas.ti code linking behaviour with social media background

the Theory of Planned Behaviour (TPB) over the other identified behavioural theories. This stemmed from the fact that:

- It incorporates three constructs that social psychology deem essential to model behaviour (Ajzen, 2005) namely, attitude, subjective norms and Perceived Behavioural Control (PBC).
- The constructs named subjective norms and PBC could be adapted to allow for a theoretical contribution within the context of this study. For example, determining one's self-efficacy (part of PBC) is based on knowledge, which in turn is informed by awareness and vice versa. Additionally, a number of studies that were analysed replaced subjective norms with social norms, so as to measure greater variance with regard to social influence.
- Personality constructs, such as those of the Big Five, could relatively easily be integrated with the original TPB.
- The combination of the above would enable this study to contribute to the field of behavioural information security.

The analysis also uncovered support for the research model constructs - a vital aspect leading to the development of this study's propositions (see Chapter 6). This was of particular importance when it came to arguments that related to the behavioural influence of these constructs. For example, Figure 2.9 illustrates the Atlas.ti network which was used to argue the behavioural influence of attitude.

Because some studies use a combination of subjective and descriptive (even injunctive) norms, these codes were combined and analysed as a single Atlas.ti network. Importantly, the resultant analysis had to support the uni-directional relationship between the construct *Social norms* and the *Intention to use Facebook Apps*. For example, the Atlas.ti codes in Figure 2.10 were used to support the behavioural influence of subjective norms, as one measured component of the broader construct social norms (i.e., the rest of the network contains the codes associated with descriptive norms). Figure 2.10 also illustrates some of the quotes that comprise the code *++attitude towards:influence of social norms*.

Further analysis also revealed support for the behavioural influence of the construct *Information security awareness*. Unlike PBC (as per the TPB), awareness encapsulated more

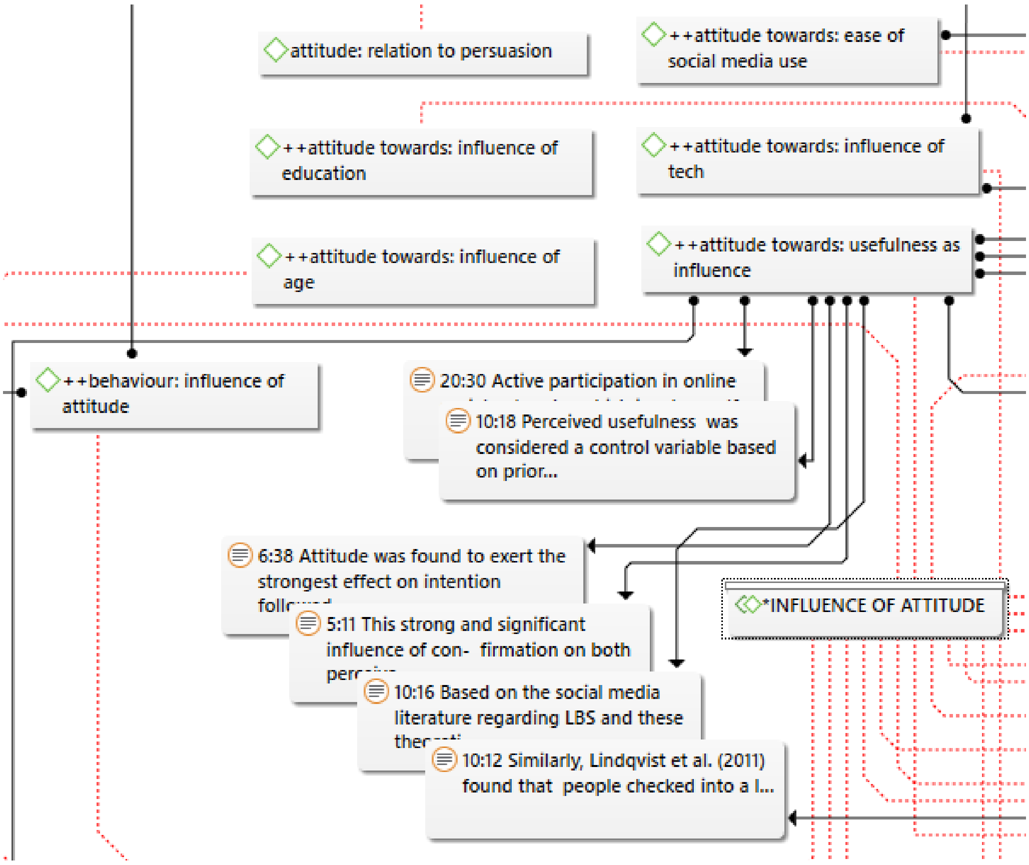

attitude: relation to persuasion
++attitude towards: ease of social media use
++attitude towards: influence of education
++attitude towards: influence of tech
++attitude towards: influence of age
++attitude towards: usefulness as influence
++behaviour: influence of attitude
20:30 Active participation in online
10:18 Perceived usefulness was considered a control variable based on prior...
6:38 Attitude was found to exert the strongest effect on intention follo
5:11 This strong and significant influence of con- firmation on both perc
10:16 Based on the social media literature regarding LBS and these the
10:12 Similarly, Lindqvist et al. (2011) found that people checked into a l...
*INFLUENCE OF ATTITUDE

Figure 2.9: Atlas.ti network used to argue the influence of attitude

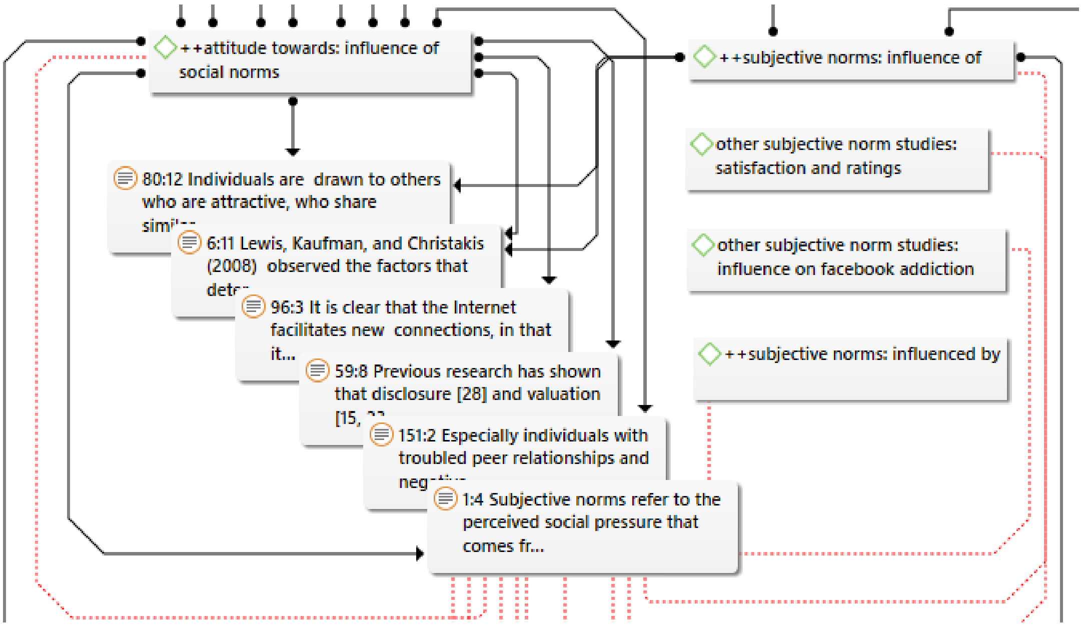
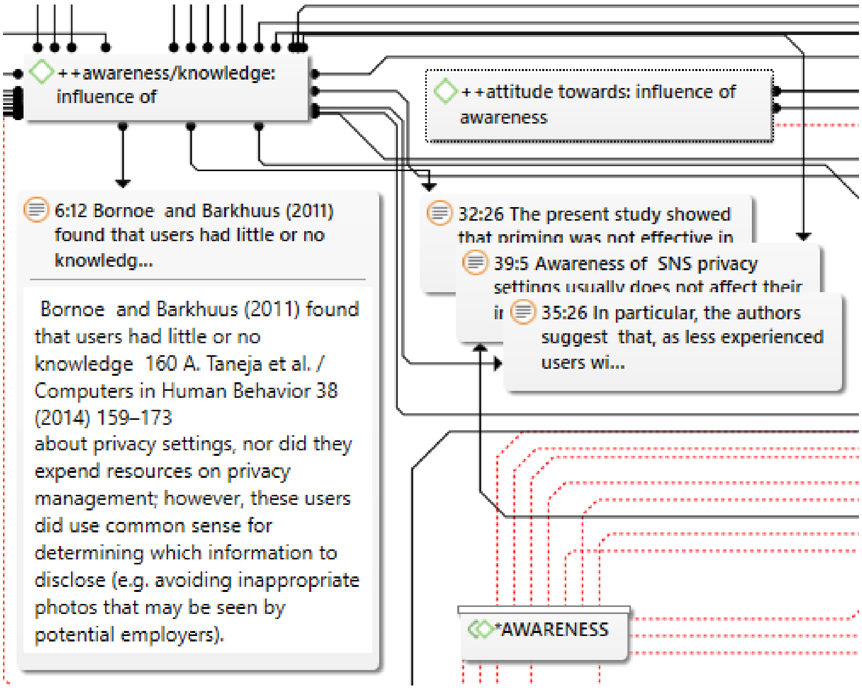

++attitude towards: influence of social norms
++subjective norms: influence of
other subjective norm studies: satisfaction and ratings
other subjective norm studies: influence on facebook addiction
++subjective norms: influenced by
80:12 Individuals are drawn to others who are attractive, who share simi
6:11 Lewis, Kaufman, and Christakis (2008) observed the factors that det
96:3 It is clear that the Internet facilitates new connections, in that it...
59:8 Previous research has shown that disclosure [28] and valuation [15,
151:2 Especially individuals with troubled peer relationships and neg
1:4 Subjective norms refer to the perceived social pressure that comes fr...

Figure 2.10: Atlas.ti network used to argue the influence of subjective norms

than just the concept of self-efficacy. Here, it was essential to find literature to support the relationship between *Information security awareness* and *Attitude towards privacy* mainly to further substantiate how awareness may increase knowledge (through learning), which in turn is required to form a sentiment and attitude (see Chapter 4). Some of the quotes used to support this argument are illustrated in Figure 2.11. These quotes were subsequently used to write sub-section 5.10, for example.


++awareness/knowledge: influence of
++attitude towards: influence of awareness
*AWARENESS

6:12 Bornoe and Barkhuus (2011) found that users had little or no knowledg...

Bornoe and Barkhuus (2011) found that users had little or no knowledge 160 A. Taneja et al. / Computers in Human Behavior 38 (2014) 159–173 about privacy settings, nor did they expend resources on privacy management; however, these users did use common sense for determining which information to disclose (e.g. avoiding inappropriate photos that may be seen by potential employers).

32:26 The present study showed that priming was not effective in

39:5 Awareness of SNS privacy settings usually does not affect their

35:26 In particular, the authors suggest that, as less experienced users wi...

Figure 2.11: Atlas.ti network used to argue the relationship between awareness and knowledge

Co-occurrence provided further confirmation of the behavioural influence of personality. For example, the code *findings:awareness* is coded in such a manner that it co-occurs with the code ++*awareness/knowledge:influence of*. Here, the quote (labelled 48:24) is associated with both of the aforementioned codes (see Figure 2.12). Through the process of inductive reasoning, such areas of overlap allowed for the identification of theoretical relationships.

As such, support for the behavioural influence of personality was obtained by inductively analysing several Atlas.ti networks, as illustrated above. One such example is illustrated in Figure 2.13, which argues the behavioural influence of personality on attitude. The resultant narrative based on the associated quotes, was used to write Section 5.3. It also provided the necessary information to create the fourth proposition of this study. Following the

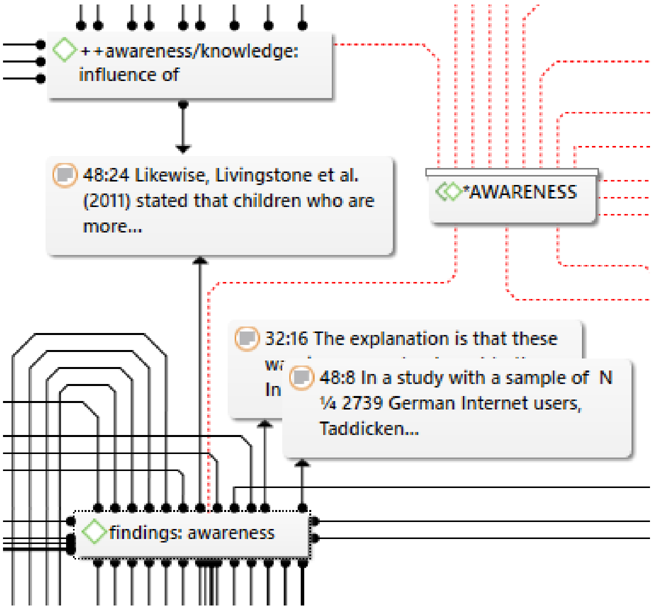
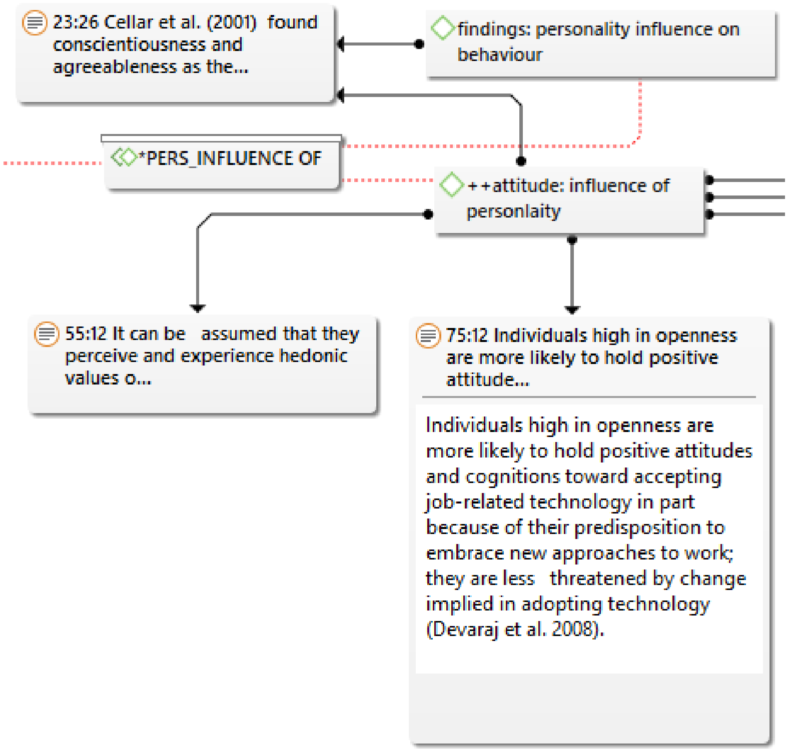

++awareness/knowledge: influence of
48:24 Likewise, Livingstone et al. (2011) stated that children who are more...
*AWARENESS
32:16 The explanation is that these
48:8 In a study with a sample of N ¼ 2739 German Internet users, Taddicken...
findings: awareness

Figure 2.12: Example of co-occurrence within Atlas.ti

aforementioned inductive analyses, four propositions were created as outlined in Chapter 6.


23:26 Cellar et al. (2001) found conscientiousness and agreeableness as the...
findings: personality influence on behaviour
*PERS_INFLUENCE OF
++attitude: influence of personlaity
55:12 It can be assumed that they perceive and experience hedonic values o...
75:12 Individuals high in openness are more likely to hold positive attitude...

Individuals high in openness are more likely to hold positive attitudes and cognitions toward accepting job-related technology in part because of their predisposition to embrace new approaches to work; they are less threatened by change implied in adopting technology (Devaraj et al. 2008).

Figure 2.13: Atlas.ti network used to argue the attitudinal influence of personality

2.7 Research instrument

This study made use of a questionnaire to collect primary data (for both the pilot and final study). These questionnaires were developed by either directly making use of or adapting items that have been used in previous studies. Importantly, it was through the process of secondary data analysis that these items were identified or developed. In some instances, multiple sources (previous studies) were consulted as illustrated in the *Source* column of the tables that list the research instrument items (see Appendix A).

Questionnaires were used from both the fields of social psychology (personality component) and behavioural information security. Moreover, they offer several advantages such as low cost, and no interviewer bias. Additionally, respondents are more comfortable to approach, have more time to complete the questionnaires, and large samples lead to an increase in the reliability of results (Kothari, 2004, p.101).

Both the pilot and the final questionnaires were structured with pre-defined response anchors aligned with the study's research questions. Additionally, all of the research model's constructs and associated items addressed various aspects of the research questions (Punch, 2003). None of the items were open-ended, making the results easier to analyse. Additionally, the sequence of the items was considered by placing easier (including demographic) items first with a clear progression towards items more closely aligned to the study's research questions. To operationalise these specifics in a manner that leads to the development of a suitable questionnaire, Punch (2003, pp.49-50) urges researchers to note the following:

- Ensure that the items align with the research questions. This was done in Chapters 4 and 5, where the literature reviews were aligned with the model's constructs, which in turn, were aligned with the research questions.

- Provide definitions of the constructs. These definitions were discussed in the literature reviews and in Chapter 6.

- Align the theoretical framework with the type of information required. For example, this study's focus is behavioural and thus it makes use of a behaviour-centric theoretical framework - the Theory of Planned Behaviour.

- Decide if these constructs will be measured by one item or several items (a scale). In this study both categorical (items measuring the number of Facebook friends for example) and ordinal constructs (those based on Likert scales) were used.
- Create the items associated with the constructs. For example, this study favoured the use of scaled responses as opposed to dichotomous (yes/no type items) responses. A scaled approach is particularly useful since it generates more information.
- Pilot the questionnaire.
- Use the pilot results to finalise the questionnaire.

Additionally, all the scaled items used five response anchors. Although a more significant number of response anchors (such as seven or nine) is likely to produce more variance, it is possible that the variance could lead to unreliability. This means that respondents are unlikely to answer in the same way if asked to answer the same questions again (Punch, 2003).

2.7.1 Pilot questionnaire

A pilot study was conducted to ensure that the proposed questionnaire is valid and reliable. It consisted of 105 items divided among the same constructs found in the final questionnaire. Several amendments were made after administering the pilot questionnaire (see Chapter 7 for these details).

2.7.2 Final questionnaire

After making the amendments above, the final questionnaire was administered (see Appendix A for a complete listing of these items). In short, every construct illustrated in the research model (see Chapter 6) is associated with a subset of the items that comprise the final questionnaire.

Of these, additional items were included relating to demographics, Facebook experience, computer experience, as well as Facebook usage. The questionnaire also included items from a social desirability scale to control for respondents over or under estimation (Snyman et al., 2017). Note that as with the pilot questionnaire, several amendments were made after administering the final questionnaire, to ensure that both the measurement and the structural models accurately fit the data (see Chapter 7 for these details).

2.7.3 Addressing measurement errors

To address measurement errors, a questionnaire's validity and reliability should be determined. Validity tests indicate to what extent the questionnaire measures what it set out to measure. For example, if a questionnaire is deemed valid, measurement differences are said to portray actual differences in respondent answers. Although Kothari (2004, p.74) discusses four forms of validity (content, criteria, concurrent, and construct) this study is primarily concerned with construct validity. To determine whether the items associated with the model constructs are valid, other propositions are associated with the results when using the questionnaire. If a correlation is observed between these other propositions and the questionnaire's actual measurements, the constructs are deemed valid.

In this study, validity tests were conducted for all the constructs (their associated set of items) in both the pilot and the final questionnaire. Principal Component Analysis (PCA) was used to test the validity of the constructs associated with the pilot questionnaire, except the five personality constructs. To assess the validity of these personality, constructs correlation coefficients (Pearson Product Moment Correlations) were used. If constructs obtained a coefficient value between -0.30 and 0.30, they were deemed statistically non-significant. Values above 0.70 or less than -0.70 were deemed statistically significant and thus valid (Gefen et al., 2000; Straub et al., 2004).

Unlike the pilot questionnaire, complete factorial validity (discriminant and convergent) was used to assess the validity of the items and constructs associated with the final questionnaire. Convergent validity assesses that the correlation of multiple items associated with the same construct is similar (Ab Hamid et al., 2017). In general, convergent validity is established when the loading values are equal to or exceed 0.50 (James et al., 2017). Additionally, the t-statistic values are required to be significant (Gefen & Straub, 2005). See Chapter 7 and Appendix A for these results and the factor loadings.

It is crucial also to assess the discriminant validity of constructs. Discriminant validity ensures that the constructs' measures (via the items) are distinct (Ab Hamid et al., 2017). One approach to establish discriminant validity is to inspect the square root of each construct's

Average Variance Extracted (AVE) value and then to compare it with the correlations of the constructs. Here, the square root of each AVE value should exceed all other correlations associated with that specific construct (Fornell & Larcker, 1981; James et al., 2017) (see measurement model in Chapter 7).

Since this study only made use of a single cross-sectional survey, the absence of common method bias also had to be established. This is especially important, given that the research model and the associated propositions were designed a priori (i.e., using literature) (Podsakoff et al., 2003). If such a form of bias is in existence, the constructs will exhibit strong correlations with each other. To asses this, the measurement model was inspected for any values above 0.9 (Pavlou et al., 2007). To formally assess the existence of multicollinearity, the Variance Inflation Factor (VIF) values were inspected for each item. Literature suggests that these values should be lower than 5.0 (Pavlou et al., 2007) (see Appendix C).

Lastly, reliability tests, which establish whether a questionnaire will produce consistent results were conducted. To achieve this, Cronbach's alpha was used for the constructs associated with both the pilot and the final questionnaire. If the Cronbach's alpha values were equal to or greater than 0.70, the construct (and associated items) was deemed reliable (Tavakol & Dennick, 2011). The reliability of the constructs associated with the final questionnaire was also assessed for composite reliability. As with the Cronbach's alpha values, a result above 0.70 indicates that the requirements for composite reliability have been satisfied (Raykov, 1997). Note that the items associated with a construct should all use the same response anchor to form part of such reliability tests.

To further reduce measurement errors - specifically, those related to respondents who are *faking good* or *faking bad* - the final questionnaire used eight social desirability items derived from the full 33-item Marlowe-Crowne scale (Ray, 1984). Note that several amendments were made with regards to the use of the social desirability scale in this regard (see Chapter 7). Measurement errors related to the measurer was deemed unlikely since these are often associated with qualitative research (Kothari, 2004). For example, an interviewer may inadvertently reorder or change his interview questions from one interview to the next. This may result in slight variations in the interview data. Of specific concern was the measurement errors related to the questionnaire itself. For example, the use of certain words may not be understood by participants or merely poorly designed.

In addition to the specific errors highlighted above, other survey errors also had to be accounted for. These are often collectively referred to as the total survey error and consists of coverage, sampling, non-response, and measurement error (Visser et al., 2000). Excluding the latter, coverage error refers to the situation where certain aspects of the population of interest are not represented in the pool from which the sample is selected.

Since this study set out to survey individuals who were effectively pre-screened (i.e., to make sure that they are United States citizens who use Facebook, and are over the age of 18), it was deemed unlikely that the sample would not contain core elements to be measured. Especially since one of the core aspects was also to measure respondent personality - something every human possesses. Random differences between the sample and the population were also deemed less of a problem, since much of these differences possibly related to personality and other individual differences, constitutes exactly what the study wished to evaluate. Similarly, the effects of non-response error were negated since the questionnaire was administered to as many qualified respondents as possible - a quota-based approach as such.

2.8 Methods used in this study

It is generally accepted that research methods fall into one of two categories - quantitative or qualitative (Saunders et al., 2016). In the latter researchers aim to gain a deep understanding of the phenomena in question. Conversely, quantitative research aims to predict or evaluate (Sechrest & Sidani, 1995) hypotheses or propositions. Since this study required the evaluation of the inductively derived propositions, multiple quantitative methods were utilised (see Section 2.8).

2.9 Primary data collection in this study

In addition to the secondary data, this study also collected primary data, which was used to evaluate the study's propositions. Primary data was collected by using the final questionnaire.

2.9.1 Sources of primary data

The source of primary data comprised making use of the Amazon Mechanical Turk (AMT) - a crowdsourcing platform that can be used for a number of purposes. One such purpose is the recruitment of questionnaire respondents. These respondents (called AMT workers) were paid a small fee to complete the survey, which was advertised as a Human Intelligence Task (HIT) on AMT. Similarly, AMT was paid a small fee for applying the sampling criteria, for providing data collection services, and for linking respondents with the questionnaire (hosted by SurveyMonkey). Several recent studies have reported using AMT in this manner mainly because it facilitates the creation of a sampling frame that is more representative of the population to be studied (Hirschprung et al., 2016; James et al., 2017; Mamonov & Benbunan-Fich, 2018). The use of AMT not only ensures demographic diversity (Tsai et al., 2016), but also avoids collecting data from only students (Lowry et al., 2016). In fact, Schaarschmidt et al. (2015, p.13) explicitly states that,

> *"...MTurk especially is suitable to conduct survey research if Internet users are the intended population."*

Additionally, Kypri & Gallagher (2003) found that the use of incentives introduced little to no effect on such results - specifically those related to web-based questionnaires.

2.9.2 Sampling strategy

A sampling strategy is defined as a specific plan to obtain a representative sample from a population - in this case, Facebook users over the age of 18 who are citizens of the United States. The strategy also provides an outline of the number of survey items (users) to be included and is determined before data collection takes place. Importantly, the selected sampling strategy needs to ensure validity and reliability by enumerating as much detail including:

- **The population type**: Here, one has to specify the items to be sampled which can either be finite (list of factory workers) or infinite (stars in the milky way). Facebook can enumerate exactly how many users are active on their platform within specific geographic regions such as those users who are United States citizens. Because this study required the participation of United States citizens that use Facebook, its population is considered finite - it changes, but those changes are reflected in the Facebook user statistics which can be calculated.

- **Unit of sampling**: The unit of sampling in this study is simply a Facebook user acting in his or her capacity.
- **Sources**: This represents the list of sources from where the sampling will take place. In this study the sampling frame comprises all the United States Facebook users over the age of 18 who are registered as respondents (workers) on AMT.
- **Sample size**: The size of the sample should not be too large or too little and is determined by the desired confidence level and margin of error. Because this study aimed to achieve a 95% confidence level with a 5% margin of error a minimum of 384 users were required (Kothari, 2004).
- **Sampling criteria**: This specifies the criteria sample items have to satisfy. For example, this study did not simply capture responses from any Facebook user, but rather those resident in the United States, over the age of 18 and active Facebook App users.
- **Sampling procedure**: This procedure outlines the specific techniques to select a sample. Selecting this procedure is vital in order to minimise systematic bias and sampling error. Systematic bias takes place when sampling has taken place incorrectly and instrument error has occurred (amongst others). Importantly, no number of additional respondents can ever compensate for this. Conversely, sampling error does decrease as the sample size increases - hence the collection of as many responses as possible in this study. In this study, non-probability sampling was employed (Fricker, 2008). Potential respondents had a choice to participate, making it difficult to calculate selection probabilities in a population that undergoes frequent changes (new Facebook users on AMT). It is acceptable to use such sampling techniques for web-based questionnaires; especially in situations where it is known that the population is not infinite, but difficult to account for or number. In such situations Kothari (2004, p.61) suggest selecting a finite number of items to represent the sample. In this instance respondents registered on AMT.

The above sampling procedure does, however, play into one of this study's limitations namely, the inability to make inferences about the entire Facebook user population over the age of 18 that are citizens of the United States. Specifically, because a non-probability approach was employed as opposed to a probability approach. It is generally accepted that probability approaches (such as list-based sampling frames) are only practically available for specific organisations and corporations (Fricker, 2008). This makes it difficult to use web-based questionnaires in a probabilistic manner.

2.10 Process of primary data analysis

Primary data was analysed using statistical methods whereby the research model constructs and relationships were deductively evaluated. To effect this process, several statistical methods were used. Once the dataset was cleaned, the data was imported into two statistical analysis software packages namely, STATA 15 and SmartPLS 3.0. Following this, the process of primary data analysis proceeded in three phases:

- The data was summarised in a manner aligned to the research model's constructs.
- Univariate (thus descriptive) analysis was performed. This conveyed the study context as well as demographic aspects such as gender, age, Facebook usage, and experience. Here, statistics were used to calculate the means, the standard deviations and the frequency distributions expressed as histograms (see Chapter 7).
- Joint analysis of the research model constructs used Partial Least Squares (PLS) path modelling. This form of analysis is often misunderstood as a means to confirm a priori causal hypotheses or propositions. Instead, it is more often used to develop a structural model that exhibits *best fit*, while taking the causal mechanisms into account (Kelloway, 1995). To achieve this, both a measurement and structural model was developed. The use of a PLS-based approach (instead of a covariance-based approach) is particularly suitable to this study, because of the development of an un-established model using data that is not normally distributed (see histograms in Chapter 7) (Hair et al., 2017, pp.34-35).

Such forms of causal inference can only be confirmed provided that certain conditions are met. One of which being that all causes of the endogenous (dependent) constructs need to be identified. Theoretically, path modelling techniques (including Partial Least Squares) are based on second-generation data analysis techniques, which test whether a structural model satisfies statistical conclusion validity (Gefen et al., 2000, p.3). In turn, this enables a researcher to perform,

> *"...a more rigorous analysis of the proposed research model and, very often, a better methodological assessment tool." (Gefen et al., 2000, p.5)*

Thus, SEM enables researchers to analyse multiple (both independent and dependent) constructs, as well as the structural and measurement aspects of the underlying research model. This makes SEM a valuable analysis framework to use when investigating real-world (thus applied) processes and their associated relationships (Gefen et al., 2000). For example, this study wishes to model the influence of five personality traits on attitude, social norms, and information security awareness. As a result, only SEM techniques can adequately investigate the different combinations of these relationships simultaneously - in this instance, to assess the overall behavioural influence when considering all the research model constructs. If the same analysis were to be performed using regression, a large number of independent analyses would have to be conducted, since first-generation analysis techniques only analyse one relationship layer at a time (Gefen et al., 2000). A more rigorous discussion as to the analysis of the primary data follows in Chapter 7.

2.11 Summary

This chapter provided an overview of how the research was conducted. Firstly, the use of a post-positivist approach was motivated, followed by a brief discussion of this study's approach to theory development. The process of secondary data collection and analysis was discussed by referring to several tables and figures to illustrate how the secondary data informed the creation of this study's research model and propositions. A survey-based methodological strategy was subsequently discussed before providing an outline of how the pilot questionnaire evolved into the final questionnaire. This was followed by a discussion on the analysis of the primary data by also providing details as to how it was collected.

This chapter concludes with a discussion about the suitability of using PLS path modelling as a means to analyse the primary data. The following chapter is the first of three literature review chapters, starting with a thorough review of the surveillance of data, both before and after the advent of mainstream social media.

Chapter 3

SURVEILLANCE OF DATA

"They who dream by day are cognizant of many things which escape those who dream only by night."

— Edgar Allen Poe

This chapter takes the form of a problem-centric review, by tracing the evolution of the surveillance of data, and making specific reference to the period after the creation of Facebook. It first gives the reader a historical overview of the surveillance of data, the outcomes thereof and provides a brief discussion of these latent outcomes, making specific reference to more recent secondary data to motivate its relevance. After a brief introduction to social media, consumerism, prosumerism and society's increasing demand for information is used as an argument as to why social media corporates have been able to both collect and misuse users' personal information. The chapter concludes by outlining how Facebook performs surveillance through their Apps - both third-party and Facebook-authored. Although this chapter refers to the concept of *dataveillance*, this is considered a somewhat narrow definition, which will instead be referred to as the surveillance of data. Importantly, Facebook App surveillance is to be considered as only one method of performing such surveillance.

3.1 Historical background

To illustrate how the surveillance of data has evolved from a mechanism to increase efficiency to an instrument of misuse, a review of the historical context is required. As a whole, the monitoring of data can be regarded as a form of surveillance. Clarke (1988, p.2) goes a step further coining the term *dataveillance* in the 1980s, which he defines as the processes that lead to,

> *"...investigating or monitoring of the actions or communications of one or more persons."*

In a follow-up article Clarke (1994) expands on this by synomising portions of this form of surveillance with the act of computer matching. Of course, here Clarke is only further addressing the *investigating* part of the definition above, since personal information on individuals is compared with the identification of new relationships. Importantly, this does not constitute a variation of the above definition, but rather an elaboration on it, since Clarke describes computer matching as a dataveillance technique. In the 1980s other authors, such as Dodge & Kitchin (2005) as well as Rule et al. (1983), also considered social intent, adding that the surveillance of data is not only performed as a means of monitoring individuals, but it is also intent on controlling their lives. These control mechanisms take on the form of bureaucratic systems (Boyes-Watson, 1994; Malcolm, 2013) that further the collection of personal information and documents in order to infer individual *actions* and *communications* from their resultant social relations with the state. As such, in these early years there existed a multitude of ways (i.e., techniques) with which corporates (or the state) could exert social control (Lyon, 2001; Smith et al., 2011) - all of which relied on the surveillance of data.

These relations were either governed by the location of the personal information or how the raw data was used. Here, the advent of computerised record-keeping made it possible to perform the monitoring activities in a consistent, reliable, and cost-effective manner (Clarke, 1988). However, monitoring was not the only reason for conducting this form of surveillance. Enhancing efficiency (Clarke, 2001a; Stewart et al., 2019), performing computer-assisted front-end verification, compiling dossiers and profiling were also commonly cited as reasons for making use thereof (Bercu, 1994; Lanier & Cooper, 2016).

The rise of databases not only facilitated the increase in efficiency, but they also made it possible to store large amounts of data (Parkinson et al., 2018; Solove, 2001). Marketing executives were able to sort and extract data in a focused manner (Bloom et al., 1994; Goss, 1995; Swanlund & Schuurman, 2016). Such focused marketing efforts reduced costs, resulting in higher success rates. Even greater success rates could be obtained by making use of geographic systems (Goss, 1995). When used in conjunction with traditional intelligence data (i.e., computer matches), these targeted individuals' profiles could be used in *segmentation* strategies allowing for their personal information to be further misused (Goss, 1995). The actual reasons for conducting such forms of surveillance could range from checking whether an individual is entitled to a government grant or because an abnormal event triggered the need to investigate a matter further (i.e., suspicion of fraud) (Batorski & Grzywińska, 2018; Kling et al., 1995).

At the time, the surveillance of data also had some positive uses. For example, retailers were able to make use of computer or data matching in order to place orders (Bloom et al., 1994) automatically, but also to strategically assist retailers (Birkin et al., 2017; Goss, 1995). Security is also listed as a use case where outright surveillance could be conducted by way of Closed-Circuit Television (CCTV), complemented by the surveillance of transactional data (Abbas et al., 2015; Clarke, 2001b). Of course, intelligence agencies were also surveilling data, although such use cases were contested for privacy reasons (Rahman et al., 2019; Shattuck, 1984). For example, at the time it was decided that intelligence data on a person could not only be useful to authorities, but also to credit bureaus and insurance brokers. Of course, all of the bureaucratic and corporate processes generated more records with which to perform computer matching at a later stage.

3.1.1 Characterising the surveillance of data

There are a number of characterisations that constituted earlier forms of data surveillance (i.e., before Facebook). For the most part, these characteristics vary depending on which year a specific article was written. The closer these articles were published to the creation of Facebook, the more prominent modern characteristics were emphasised. Not only were the actual technologies used, but also the role of social control and information capitalism (Lyon, 2001).

Even in the late 1980s, authors, such as Clarke (1988) were able to characterise the surveillance of data as an activity that completely removes that which makes us individuals, replacing it with a notion that upholding the state is of greater importance. Collecting and searching for evidence through the surveillance process assisted state entities in identifying those individuals of specific interest (Kling et al., 1995; Shattuck, 1984). In this manner, computer matching was performed with the intent to identify individuals before any evidence was presented. Common amongst such uses was the search for individuals who had committed fraud (Clarke, 2001b). As such, the presumption of innocence is replaced by that of guilt (Shattuck, 1984). Moreover, these *matches* were often removed from the context in which they were collected (Byrne, 1995) - thus aiding incorrect conclusions (Shattuck, 1984). This form of surveillance was thus akin to that of a process which indiscriminately matched personal information with the intent to categorise or label; a means of social sorting (Eastin et al., 2016; Lyon, 2001) to facilitate the decision-making process. For example, such surveillance processes might be used by an insurance company to compile a risk profile of a potential client.

These decision-making processes also emphasised how the surveillance of data changed. Once relegated to only being used by single state entities, corporates and governments could now integrate disparate sets of data (Lyon, 2001). Facilitated by the increasing use of distributed databases (O'Brien & Yasnoff, 1999), networking (Bennett, 2001; Palmer, 2005) and a reduction in operational costs, surveillance efforts could now leverage concepts, such as natural language queries in order to extract data from these disparate (but also decentralised) data sources (Apostolou, 1988; Nam, 2017). Personal information could now be collected for one specific purpose (taxes for example) and then *matched* with data gathered for other reasons (Byrne, 1995; Shantz, 2018); a case in point being the Financial Crimes Enforcement Network (FinCEN). Here, seemingly unrelated pieces of information were aggregated towards creating new information that would not have existed before (Bercu, 1994).

It is this flexible use of data that made it difficult to ascertain the various sources of the actionable data (Bennett, 2001). The rise of indirect social relations typified by our interactions with corporates and the state created a wealth of documentary records (Murray & Fussey, 2019; Rule et al., 1983). As more of these records started to capture events of importance, the more this form of surveillance became a hegemonic instrument (Goss, 1995; Reeve, 2019).

As such, government organisations were able to leverage public databases in order to supplement their own records on individuals of interest (Boyes-Watson, 1994; Lodder &

Loui, 2018), whilst corporates were able to leverage the growth of the Internet (Solove, 2001), in order to sell and buy personal information. Note that such transactions did not always involve capital in the traditional monetary sense, but instead relied on individuals to voluntarily supply their personal information with the understanding that they would receive some sort of benefit in return (Boyes-Watson, 1994; Jai & King, 2016).

3.1.2 Forms of data surveillance

As outlined by Rule et al. (1983), the surveillance of data was traditionally concerned with the monitoring of individuals by means of data recorded on physical documents. However, as technology progressed, the focus shifted to the surveillance of data in electronic format. In fact, one type of surveillance takes place by accident, as is the case with information security breaches (Bennett, 2001; Sert et al., 2015). Although not always intentional, these breaches had the same effect as any other, namely the opportunity to view data indicative of another individual or organisations' actions. Bennett (2001) continues, stating that these incidents were likely to increase as the underlying technologies increased in complexity.

Another form of data surveillance was the unintended consequences when using applications not intended for surveillance purposes (Bennett, 2001; Fink et al., 2015). A case in point was the Intel Corporation who imprinted each Pentium 3 processor with a serial number that could be queried remotely via web browsers. Other forms of unintentional surveillance relate to the entry and exit logs created when entering so-called *smart buildings* as well as the associated usage patterns when monitoring these logs. In extreme cases, this information could be used to ascertain how many occupants were in a building in a given time period. In turn, raising issues related to the privacy of personal information.

Unlike the unintentional forms of surveillance, intentional surveillance makes use of specific applications to achieve their surveillance goals. It constitutes a direct and deliberate move by an individual or organisation to monitor the actions of either themselves or other individuals. Examples include the installation of spy software on mobile devices and home-based webcams. Studies specifically mention the use of a product called *Spector* (circa 2001), used to monitor homes from the users' desktops (Bennett, 2001; Wolfe, 2017). Initially intended only to perform baby or nanny monitoring functions, it soon morphed into an elaborate monitoring platform capable of logging keystrokes, snooping passwords and profiling general use of the desktop it was installed on. Some online directories that allowed indexing and searching based on incomplete information could also be used to locate and profile individuals. These later evolved into dedicated surveillance-based websites with which a subject could locate groups of individuals - gradfinder.com being one such website (Bennett, 2001).

A more complicated form of data surveillance is that of surveillance by design. At the time, companies, such as *Doubleclick* provided private enterprises the ability to buy advertising space on websites in the form of banner ads (Bennett, 2001; Palmer, 2005). At the time, *Doubleclick* made use of sophisticated software that analysed individuals' browsing habits, noting which websites were visited as well as the frequency and duration of such visits. This allowed *Doubleclick* to match the constructed profile with a suitable ad to be placed on the websites visited by that specific Internet user. During the early 2000s advertising companies also started making use of *Web Bugs*, now referred to as *Spyware*. As the name suggests *Spyware* also tracks an Internet user, but does so via a locally installed software program. It is important to note that the actual *Spyware* software is often embedded within other software programs, without the user knowing about it (Harkin et al., 2019). Here, Bennett (2001) uses the example of the *Desktop Media Network (DMN)* that (circa 2001) controlled advertising from within about 500 desktop applications. This enabled DMN to reach about 8.5 million potential consumers at any given time. Other intentional forms of data surveillance included *GIF trackers*, which could be embedded within websites, documents and e-mails, as well as copyrighted information (Frackman et al., 2002). Such forms of surveillance made it viable for corporate and government organisations to not only gain an understanding of how the aforementioned electronic artefacts changed hands, but also the user involved.

Although the earlier definition of dataveillance covers its intent to monitor the actions of users, it does not articulate the underlying motives thereof. From the preceding discussions on the various characteristics and forms thereof, it is possible to gather that there may be several reasons why it was conducted. Notably, many of these forms of surveillance were either conducted without the user knowing about it (via *Spyware*) or the information was sold to a third-party without the user being informed of the sale (Bennett, 2001). Some corporates did not even consider a user's Internet activities as something that belonged to them (Bennett, 2001).

To illustrate this, consider an e-commerce merchant's customer list, which technically belongs to the merchant, although the data is not related to the merchant. E-commerce merchants, such as *Amazon.com* realised this early on and included this in their privacy policy (Bellman et al., 2004; Bennett, 2001). As such, any subsequent sale of customer information is covered by acceptance of this privacy policy. However, it does not change the fact that such merchants financially benefited from the sale of this information. The only thing that has changed is the fact that the user is aware of such practices. There is no real alternative; hence the sale of personal information, whether it is unintentional or by design is understood as a universal truth; a fetishism in the Marxian sense (Fuchs, 2011). Before furthering this argument, a more elaborate discussion on the various enablers of this form of surveillance is required.

3.1.3 Enabling the surveillance of data

For the most part, this review highlighted two core enablers. One is technological and the other is related to the absence or negligence of privacy legislation (Culnan, 1993; Liu & Fan, 2015; Pincus & Johns Jr, 1997). Since this study is not making a legal argument, the resultant discussion will only briefly touch on such legalities. Nonetheless, many of the articles within the literature alluded to the fact that not only technology, but also legislation, has played a significant role in the rise of the surveillance of data. Some articulate specific techniques (Formanek & Tahal, 2018; Tavani, 1999) as well as how the progression of technology has influenced such surveillance practices. It is the objective of the following section to discuss some of these technological enablers.

3.1.3.1 Technology

For the most part, it seems that these technological enablers were evolutionary in nature. For example, Clarke (1988) mentions six key Information Technology (IT) developments that made it possible to start storing and processing large amounts of data cost-effectively. Here, Clarke makes an important observation, stating that for the first time a wide range of technologies with individual uses, were combined towards achieving something larger than the sum of the individual parts (General Systems Theory as such). Driven by an initial commitment to administrative efficiency, information privacy was relegated to something worth noting, as long as it did not interfere with said efficiencies. To support this, personal and organisational data would have been stored centrally. This prompted a proposal to construct a national data centre in the United States, which was denied because of information privacy concerns; notably the ease of information retrieval from such a central repository (Clarke, 1988). Unlike the 1960s, a central repository of information was no longer required in the late 1980s. However, this only applied if:

- An array of systems processing data for a specific reason exists,
- These systems are linked to each other by at least one network, and
- The resultant data is always identifiable.

Nonetheless, the surveillance of data still suffered from being unable to identify data in a consistent manner across a variety of systems. Thus, because organisations made use of a variety of systems, it was hard to match data belonging to the same person across a myriad of information systems (Clarke, 1988; Dornan & Hudson, 2003). In turn, this prompted the creation of multiple or general use identification schemes, making surveillance easier to conduct. Some of the technologies that facilitated this included cheques embedded with magnetic ink (Clarke, 2001a), which made it possible to consistently and accurately process large amounts of cheques from a variety of banks.

From a communications perspective, technologies such as caller-id could be used to facilitate looking up the details of individuals when combined with online directories (Bloom et al., 1994). Internet usage is also regarded as an enabler, mainly because it assisted corporates in their monitoring activities, such as spying on their employees' e-mails and web usage (Clarke, 2001b; Rajamäki et al., 2012; Robbin, 2001). For example, Clarke states that it is not uncommon for organisations to have used such technologies to conduct surveillance on individuals who they have a vested interest in. Hence, employees were often subjected to some form of data surveillance (West & Bowman, 2016). The usage of other systems, such as telephone networks was also used as a means to not only track individuals, but also to comply with mandates regarding data gathering for intelligence agencies (Mayer et al., 2016).

In addition to Internet usage, subversive tracking of individuals was also perpetrated by means of interrogating their *clickstream data* (Solove, 2001; West, 2019). Such technological mechanisms relied on the ability of websites to track what an Internet user does while browsing. Items of interest included the name of the Internet Service Provider (ISP), the Internet Protocol (IP) address, the specifications of the host and which website the user used to navigate to their current location (Solove, 2001). These insights not only described the current Internet user's operating environment, but also allowed corporates to compile detailed profiles (Parkinson et al., 2018; Solove, 2001).

Another use of the *clickstream data* was to store the information on the localhost, by making use of *cookies* (Clarke, 2001b). These *cookies* also tracked a user's Internet usage (Gotterbarn, 2016), but were more sophisticated in that they could relay accurate tracking information even though a host's IP address had changed. This made it a more robust means of performing surveillance, since it was able to function even if a user made use of privacy-enhancing technologies, such as Virtual Private Networks (VPNs).

Similar functions could be performed by *web crawlers* or *spiders*, which anonymously trawled websites looking for specific information (Desai et al., 2017; Gotterbarn, 1999). Once found, the information is sent back to the website or host and saved within a database. The *spider* then continues its journey by navigating to all the linked websites where the process is repeated (Lyon, 2001). Unlike these *spiders*, Tavani (1999) describes the use of software agents, such as intelligent autonomous agents, that are able to intelligently search through websites in order to uncover patterns of interest linked to certain individuals (Desai et al., 2017).

Once corporate or government organisations have amassed a substantial amount of information (as described above), they had the option to use data mining in order to make inferences from data which had not previously been possible (Tavani, 1999; West, 2019). Although data mining was often used within a single database, discovered relationships and matches may not have been apparent at first (Rao et al., 2018). Furthermore, as personal computers became increasingly powerful, they too performed data mining (Kling et al., 1995). The argument here also hinges on the fact that data mining facilitated monitoring the actions of individuals and groups. It differs from computer matching in that its primary aim was to infer or to create information regarding groups of individuals rather than starting with a preconceived idea of the interesting group (Rao et al., 2018; Tavani, 1999).

As a by-product of the use of technology, transactions also facilitated the process of conducting surveillance of user data (Lyon, 1992; O'Dwyer, 2019). This was brought about by the increased use of electronic systems (now even cryptocurrencies) for banking, in lieu of traditional forms of payment, such as cash (Clarke, 2001a; Shapiro, 2019). Instead, individuals were now able to make use of automatic teller machines and *loyalty schemes* (Cecez-Kecmanovic, 2019, p.217).

In the 1990s the use of debit cards, electronically transferring funds (Gray, 1989) and monitoring the sale of properties (for tax purposes) (McCrohan, 1989) allowed for even more transactional growth, with many individuals making use of these cards to make the bulk of their day-to-day purchases (Clarke, 2001b). Soon financial organisations started to ally themselves with other corporates in that they either sold their customer information or bought information from other corporates (Mascarenhas, 1995; Singh & Singh, 2015). Similarly, automatic ordering systems, automatic dialers, Videocarts and videotext (Bloom et al., 1994) facilitated the gathering of transactional data directly related to orders of a specific product which assisted marketing organisations in creating purchasing profiles themselves (Bloom et al., 1994; Ruckenstein & Granroth, 2019). These profiles were then used within expert systems, such as NEGOTEX and FinCEN, which were used in the 1990s to aid marketers to profile individuals financially. Transactions generated in the maintenance of indirect social relations with government organisations, such as the Federal Bureau of Investigation (FBI) and the Internal Revenue Service (IRS), also facilitated the surveillance of data (Stahl, 2016).

Purchasing profiles could also be created by geographic information systems, that assumed that individuals with similar social values tended to live in the same neighbourhood. Based on an additional assumption that these individuals could be represented by the same purchasing profile, organisations were able to market within that geographic area (Goss, 1995; Wood & Mackinnon, 2019). With the advent of biometric and chip card systems, organisations were able to track the movement of individuals in real-time, without relying on geographic systems only (Neves et al., 2016).

Together, these technologies formed the pinnacle of consumer profiling (circa 2001), which literally tried to manage and measure individual consumption scientifically (Goss, 1995). The more these individuals consumed, the more detailed the psychographic data became (Goss, 1995; Lyon, 2016). This enabled corporates to understand their consumers better, which allowed them to develop more products for consumers (Goss, 1995; Maulana, 2019). In turn, this led to not only the reification of consumerism, but also furthered the capitalist agenda of generating more profit with less capital outlay; all enabled by the surveillance of user data (Briziarelli & Flores, 2018; Fuchs, 2011).

3.1.3.2 Legislation

A review of the surveillance of data warrants some discussion on the legislative reasons why it became a popular means of capitalising on personal information. Here, legislative arguments mainly revolve around the concept of personal or information privacy; especially the slow decline in terms of the importance placed on an individual's right to privacy. For example, even though a 1977 commission made 155 recommendations regarding fair information practices, only a few were adopted (Kling et al., 1995). Two years later, it was suggested that the cost of computer matches be calculated, in addition to giving notice (to the American Congress) before proposing matches between data sources hosted by more than one department (Apostolou, 1988).

This meant that United States organisations were only required to publish their intentions regarding the latter inter-departmental matches. Further regulation with regard to these matches were not adopted, since it hampered the legitimate flow of information between organisations that do not reside within the same geographic region (Clarke, 1988). Having said this, somce legislative measures did attempt to level the corporate playing field from a legislative point of view (Nissenbaum, 2018). For example, collaborative efforts were undertaken to ensure that individuals' personal information were not abused via the matching process. Nevertheless, a number of corporates felt that such global views of information privacy and the related legislation was not in their best interest (Byrne, 1995). Byrne (1995, p.56) elaborates on this stating that,

> *"Antiquated and unenforceable privacy laws succumb to electronic supply and demand, regardless of possible harm to others."*

According to Lyon (2001), although there were legislative controls regarding the secondary use of personal information, they lacked oversight and were not comprehensive, insofar that consumers were still required to provide some information in order to receive services (Korff et al., 2017). In those instances, individuals were faced with the same ontological dilemma raised by Fuchs (2011). They were forced to comply, since there was no real alternative other than not receiving the service.

Admittedly, a Facebook account is not a critical service (a modern metaphor), but there were other services, such as a bank account (traditional metaphor), that were difficult to avoid in order to perform within society. Boyes-Watson (1994) added to this argument, stating that although there were protection measures for the provided information, these were inadequate due to the voluntary nature of participating and enforcing such measures. As an example, O'Brien & Yasnoff (1999) stated that a study conducted in 1999 showed that only a fifth of state health organisations in the United States required individuals to give consent when collecting health-related information. Additionally, a third of the surveyed state health organisations not only prohibited individuals from viewing their personal information, but also had no means of actually correcting data that was incorrectly captured. Similarly, Solove (2001) viewed the problems regarding information privacy not as laws that needed to address exploitation after it had taken place, but rather legislation that allowed for the regulation of technologies (such as data mining) (Yoon et al., 2015). This theoretically prohibits even starting the information discovery process. However, even this approach was problematic, since privacy legislation (circa 1999) only applied to the transfer of information between databases and since data mining mostly took place within a single database, this did not adequately address the problem (Gudivada et al., 2015; Tavani, 1999).

Anti-piracy legislation also enabled corporates to legally conduct surveillance of data, in order to locate individuals guilty of copyright infringement (Clarke, 2001b). Here, technologies, such as *GIF trackers* and *cookies*, facilitated surveillance efforts. Furthermore, many of these surveillance practices were conducted as clandestine operations, making it a difficult problem to address with appropriate legislation (Baker et al., 1986; Lichy et al., 2017).

The latter instance of surveillance briefly highlighted some of the legislative reasons why the surveillance of data was able to thrive. For the most part, many of the legislative efforts to address information privacy had to contend with several assessments conducted by privacy scholars (Westin & Baker, 1973; Westin, 1971) who initially had no qualm about elaborate data surveillance mechanisms. Instead, the emphasis was placed on regulating it in such a manner that it not only became more socially acceptable, but also legally justified (Bennett, 2001). To a large extent this is still the case (Pavone et al., 2018).

3.2 Outcomes of data surveillance

It is worth noting that the outcomes discussed here are similar to the reasons for actually conducting surveillance of data. Although not alluded to in the literature, some of these outcomes are latent in nature. If anything, it is the operationalisation and resultant social and economic manifestations that shape these latent outcomes. It is understandable that corporates strive to gather more capital and that government organisations wish to combat terrorism as well as fraud, but collectively, the literature implies more than just these specifics. In this section, the discussion will flow from a direct view of both the positive and negative outcomes of data surveillance culminating in a discussion on one such latent outcome, namely, social control.

3.2.1 Positive outcomes

One positive outcome cited by a number of authors (Brayne, 2017; Clarke, 2001a; Gray, 1989; Lyon, 1992), is the increase in administrative efficiency. Another positive outcome is a general increase in awareness with regards to how and where personal information may be stored (Gray, 1989). In turn, it is this increased awareness, which allows IT professionals to question such surveillance practices as well as the subsequent infringements or legislative shortcomings around the privacy of personal information (Clarke, 1988; Snowden, 2016). For example, such surveillance practices made it possible to locate individuals who did not pay their taxes (Baker et al., 1986). Using an approach that monitored a variety of transactions, these organisations were able to identify and track individuals engaging in drug trafficking as well as illegal immigrants and fraudsters (Boyes-Watson, 1994). It is still used for these reasons (Keiber, 2015).

From a corporate perspective, the use of geographic information systems is also reported to have reduced the amount of unwanted advertising material, since these forms of surveillance enabled corporates to engage in cost-effective marketing campaigns that only targeted specific geographic regions (Goss, 1995; Jayaram et al., 2015). Similar marketing strategies were also used by the medical industry who are required to be able to follow groups of individuals over an extended period of time (McCrohan, 1989). This is also still the case (Ball et al., 2016).

3.2.2 Negative outcomes

Although the negative outcomes were briefly discussed, the historic persistence (Westin, 1968) and resultant literature analysis, warrants a further discussion on the specifics. In this regard, the literature is replete with examples where the surveillance of data has been conducted, resulting in the misuse of personal information.

In some instances such forms of misuse takes place intentionally (McCrohan, 1989); albeit under the guise of market liberalism (Byrne, 1995). For Mascarenhas (1995), the combination of seemingly disparate pieces of information is largely an unintentional effect of using technologies capable of finding and matching personal data where collecting the individual pieces may not impinge on the privacy of that individual, but rather the combination of these pieces of information (Murphy, 2015).

In this study, this is referred to as *misuse by transformation*, since on its own the information is harmless, but results in misuse when combined (thus transformed) with other seemingly unrelated pieces of information. This is especially true of data mining and to some extent databases (Salloum et al., 2017; Solove, 2001), where both the operators of the mining software and the individuals under scrutiny, are unable to determine what information the mining processes will uncover (Tavani, 1999). Not only is the information open to transformation, but also interpretation. In some instances, some of these interpretations may be incorrect (Bennett, 1991) or falsified (Bloom et al., 1994), fostering the growth of illegal trade in personal information (Boyes-Watson, 1994); irrespective of whether or not it is accurate.

These transformations and associated misinterpretations could also be misused in such a manner that it causes financial harm by denying certain individuals a service to which they are entitled, as was the case with welfare grants in Massachusetts (Bozeman & Bretschneider, 1986). It is even possible for such a misinterpretation to permanently affect an individual's ability to apply for credit or insurance, since there are no mechanisms to find all the incorrect copies of this information; hence the possibility that this incorrect information may persist (Lyon, 2001; Turow et al., 2018).

However, not all misuses rely on transforming or interpreting personal information. Such forms of misuse take the form of aggregated information that is categorised and used in that form (Bloom et al., 1994; König, 2016). These uses vary depending on the immediate motivation, which in the case of Blockbuster Video (circa 1989) became a misuse of information derived from the categorisation of aggregated rental data. Similar activities, usually conducted by information brokers (Byrne, 1995), started to blossom in the late 1980s allowing for the categorisation of individuals by means of interrogating public information systems.

It is important to note that the interrogation of public information sources still takes place (Araujo et al., 2017), but should be seen in a different light as that of a database or data warehouse in that the operations that take place in the latter is obscured from public scrutiny (Tavani, 1999). Although information privacy studies, such as the one conducted by Culnan (1993), aim to understand what types of personal information is most sensitive, they also contribute to the problem of categorisation by providing detailed categories of information (Boo et al., 2015; Fukuta et al., 2017).

The value of the harvested personal information also features within the literature. Such forms of information capitalism is centred on the idea that large corporate databases contain a myriad of information that is valuable not only in its own right, but also because it is valued by others (Solove, 2001; Zuboff, 2015). In the traditional sense, recorded information usually consisted of facts that most organisations kept track of, such as a name and surname or identity number. However, as technology progressed even the data about an individual's data or online behaviour (the *clickstream* data) became valuable and was often sold as a commodity (Bennett, 2001).

Since these activities were conducted without the knowledge of the users, it also constitutes a misuse of personal information. Such forms of surveillance are as nefarious as it is profitable (Singh, 2018), with only five national marketing databases containing information on almost all of the households in the United States in the early 2000s. Unlike, the 18th and 19th century, creditors in the 20th century were not able to personally get to know the individuals they are extending credit to (Solove, 2001). As such, the need arose for third-party credit checking companies who go about collecting as much information on individuals so as to be able to sell this information to other corporates who would like to know the risk profile of a potential customer (Solove, 2001). Other forms of misuse include the latter use of banner advertisements, which made indirect use of the *clickstream* data in that it was used to create a detailed browsing profile of a user. This, in turn, enabled the advertising company to select an appropriate ad to display on websites frequented by that user (Kang, 1998). As such, it is not the *clickstream* data itself that becomes a commodity, but rather the resultant profile created from the *clickstream* itself.

3.2.3 Social control

Unlike the visions of George Orwell, technology has not been used to advance the surveillance of data at the behest of some totalitarian regime (Clarke, 1988). Rather, as the literature suggests, this was an opportunistic move on the part of not only the government but also corporates (Goss, 1995; Rogers & Eden, 2017). As time passed, more and more of the corporates realised that individuals have minimal means of resisting these practices and even if they did, the problems were soon addressed followed by an enhanced and better means of conducting surveillance of data (Goss, 1995; Uldam, 2016). According to Goss (1995, p.193),

> *"The consumer, whether naive or sophisticated, is thus bound up within this dialectic of social control."*

To measure the progression of the surveillance of data, consider that only one matching program was actively used in 1977 (for welfare grants). In 1985 this number had risen to over 500 matching programs even though the United States Privacy Act of 1974 condemned, such actions (Gray, 1989). If one views this together with the fact that the information is owned by those who collected it, individuals have slowly been losing control of their personal information (Kling et al., 1995).

Similar issues were explored by Lyon (1992), who refers to this type of surveillance as *the new surveillance*. For Lyon this type of ubiquitous surveillance laid the foundations of what was to follow, which included serious issues regarding social control. Clarke (2001a) highlights one such issue calling it the *soft sell* (p.220). This implies that governments and corporates first introduce (or sell) the public a morally acceptable solution to a social problem, which could be leveraged to increase their level of control as they slowly introduce less morally acceptable solutions to the same problem. So the cycle continues until all these moral barriers have been rendered obsolete.

To further illustrate this, Clarke (2001a) uses the concept of tracking, which he states was first introduced as a means of locating pets. However, as of the early 2000s tracking pets and livestock in this manner is not an issue; hence, the move to try and track humans (specifically children). Of course, this type of tracking is a form of social control; albeit indirect, since those being tracked can still use free will. What it does introduce is the sense that this is an acceptable form of surveillance.

A related form of social control is the trail of transactions when individuals make use of ATMs and point of sale systems (Clarke, 2001b). Again, this qualifies as an indirect form of social control derived from the use of systems that are prohibitively expensive, and thus only operate under direct control of corporates and governments (Marx, 2001). For example, it became possible for banks to track the movement of their customers by analysing ATM usage patterns (Clarke, 2001b). In addition, they could also control how frequently a customer had to visit a bank branch in order to renew a debit/credit card, or to update personal information. For these reasons, the everyday life of individuals became increasingly repressive and controlled; specifically by governments (administrative reasons) and corporates whose only intent was to further their capitalist agenda (Goss, 1995). As such, governments and corporates controlled not only the actual information of individuals, but also the means to acquire more, if so desired. As such, these two entities exercise social control, via the surveillance of data, in such a manner that they are,

> *"...always a means to power." (Goss, 1995, p.166)*

In the preceding sections, a brief overview of the surveillance of data was presented (i.e., those conducted in the era pre-Facebook). For the most part, these discussions highlighted themes that were more semantic than latent, with the exception of the section detailing its controlling nature.

3.3 A retrospective synopsis

It is anticipated that a similar review focused on the surveillance of data conducted after 2004 will be filled with the same themes as already presented. Post-2004, most of these themes are only amplified by technological progress with much of the underlying themes (such as social control) having existed for many years prior. What this historical discussion has illuminated, however, is the technological progression, which ranged from barely using technology as a means of surveillance (in the 1970s), to the realisation that the use of technology is the only plausible means of conducting surveillance efficiently and economically (towards the late 1990s). It is also clear that such surveillance practices spawned a number of retroactive inquiries regarding the privacy of information, mainly because technology outpaced legislation in this regard. For the first time the concept of information privacy had to be understood not only in terms of what it is (i.e., from a philosophical point of view), but also the implications of such surveillance practises on users' personal information.

Instead of focusing on the moral and ethical issues that surround the surveillance of data, individuals are segmented, profiled and categorised so as to be bombarded with targeted marketing material or other efficiencies, which effectively *sells* the idea of surveillance to the public (Clarke, 2001a). From a technological point of view, this has not been a difficult sale, since much of the surveillance practices in the late 1990s were conducted without the relevant individuals being aware thereof. In turn, this has perpetuated the belief that the surveillance of data and its related practices are benign and primarily conducted to enhance one's life.

To further bridge the gap between this historical view of data surveillance and social media, Fuchs provides a number of critical perspectives. Fuchs (2017), in his critical appraisal of social media, provides credible support for his argument that communication technologies (as used above) are deeply entwined with both globalisation and capitalism. Starting with IBM who sold punch cards to the Nazi's Fuchs provides a detailed account of just how much of the computer industry (as well as the Internet) can be attributed to corporates' desire to accumulate more capital.

The earlier review touched on some of these by highlighting how corporates used not only legislation, but also communication technology to their advantage in this regard. For example, some of these technologies enabled the construction of more extensive networks, which in turn facilitated the creation of online communities, namely, bulletin boards (Fuchs, 2017). Using the basic communicative premise of bulletin boards in conjunction with the fundamental human desire to interact socially, a number of prominent social media services were spawned post-2004.

3.4 Introducing social media

Having outlined the surveillance of user data pre-2004, the rest of this chapter provides an outline of precisely how and why the surveillance of user data takes place on social media (i.e., after the creation of Facebook). It culminates with a discussion describing how the surveillance of social media-based data (using Facebook as an example) has become problematic in contemporary society, by providing direct alignment with the problem statement contained in Chapter 1.

At this point, one may ask, what is social about a social media service? To a large extent, this depends on how the user interacts with the media in question. This study is as much a creation of individual cognition (on Facebook App surveillance) as it is a synthesis of other authors' cognition on this topic. For example, this study draws on a number of disciplines (over decades) - most placing an emphasis on social interaction and cognition. It is this social interaction which subsequently leads to the formation of connections.

Cultural values, the ideas of others within one's circle of influence, and one's own perceptions about self-efficacy directly influence the behaviours that result from interacting socially. Using Hegelian dialectics, one could formalise these processes as the interplay between social cognition, communication, and co-operation. Thus, from a philosophical perspective, social media could be viewed as a,

> *"...dynamic threefold process, in which, based on subjective cognitive processes, social relations emerge (communication) in which new systems and qualities can be formed (co-operation)." (Fuchs & Trottier, 2015, p.114)*

If one were to think about the behaviour that emerges as a result of this interplay, one may realise that it culminates in not only the production of tangible elements (a car for example), but also those intangible in nature (information). These elements are imbued with the ideals and shared beliefs of those involved in the production process; thus leveraging a shared ideological worldview.

As such, social media allows users to utilise Web 2.0 technologies towards the creation and sharing of content amongst users with similar worldviews (Chen et al., 2016; Li et al., 2015). For Albrechtslund (2008) it is this very feature that researchers should consider before claiming that the surveillance of social media-based data is an inherently negative practice. The very nature of social media requires a certain degree of surveillance to take place, which Albrechtslund refers to as a participatory exercise. Here, users voluntarily share a number of personal aspects of their life, thus connecting users with similar interests and views on life.

From an academic perspective, there are numerous definitions of social media. One such definition by Boyd & Ellison (2007, p.211) states that social media could be viewed as,

> *"...web-based services that allow individuals to (1) construct a public profile or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system."*

It is precisely these connections that allow social media users to socialise and grow their circle of influence (Correa et al., 2010). Such growth requires the transfer of information which typically involves sharing content; either created by an individual user or with other users, as an act of co-creation (Hughes et al., 2012). In turn, this focus on the social aspects of online communities has increased the popularity of social media platforms, with over two billion users accessing a social media service on a daily basis (Koban et al., 2018). In fact, social media has become so pervasive that many users regard it as a crucial part of their life (Marino et al., 2016; Vladlena et al., 2015), which is clearly illustrated by the exponential growth of Facebook (amongst others) in Figure 3.1.

Importantly, it is regarded as a vital component of modern psychosocial development (Hallam & Zanella, 2017). Users browse through the profiles of others to stay abreast of new developments within their social circle, whilst internalising the information using their unique psychological profile (Jordaan & Van Heerden, 2017; Kuem et al., 2017).

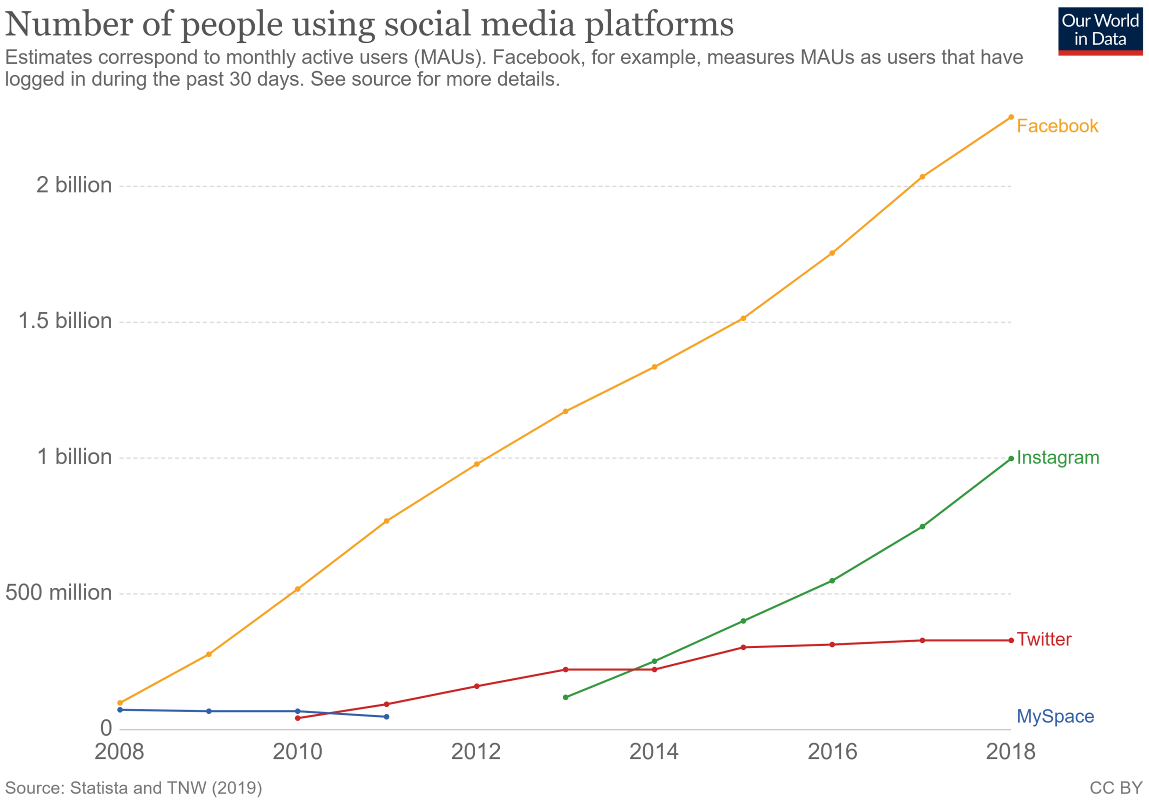


Figure 3.1: Growth of social media (adapted from https://ourworldindata.org)

Efforts to internalise such social interactions can take place in a number of places. For example, Kaplan & Haenlein (2010) state that there are six forms of social media services namely:

- Co-created and collective projects, such as Wikipedia,
- Platforms that facilitate blogging including Twitter,
- Online communities centred around specific content, which includes the likes of YouTube,
- Social networking sites, such as Facebook,
- Online multiplayer games (i.e., World of Warcraft), and
- Virtual worlds that facilitate socialising, like Second Life.

Given that these services cover such a wide range of social interaction, it has been suggested that their everyday use has (and still is) changing the dynamics of social interaction; so much so that it also impacts life offline (Hallam & Zanella, 2017). In fact, Fuchs (2017) goes so far as to suggest that these social interactions form a core component of modern communication; one without which we cannot survive. In this regard, when sharing world-views, users form online communities that allows them to feel a sense of belonging. This further fuels the popularity of social media services, making them particularly appealing to the corporate nature of some of these services.

3.4.1 The "corporation" that is social media

Dominated by capitalism, the modern economy is heavily focused on the production and consumption of information (Fuchs, 2017). Unlike previous years where most information could only be found in books and libraries, individuals now have access to a plethora of information by way of the Internet. This has led to an increase in the demand for information. Often referred to as the information economy (Schwartz, 2017) the current economic climate has enabled social media corporates, like Facebook, to make the appropriation and sale of personal information their primary business model (Marichal, 2016).

For example, a significant aspect of Facebook's business model revolves around advertising, which is used to argue that the creation of content by users and the resultant communication to view said content, results in the creation of surplus value. It is precisely this surplus value, and the consumption of the resultant content, that makes it possible to classify Facebook users as prosumers (Fuchs, 2011). In this context, these users and their associated content is sold as a commodity, with the fundamental difference being that these users, unlike, traditional mass media audiences, create and consume the commodity. This is further compounded by the fact that social media corporates use their privacy policy to obscure the extent to which such user-generated content is sold to marketing corporates. Instead of explicitly stating that the content is sold for profit, they merely indicate that it may be *shared* with third parties to improve their services.

Where capitalism was once dominated by paid labour, this form of prosumer capitalism has introduced concepts such as unpaid labour (often also pleasurable) with many prosumer-based products being offered free of charge (Facebook services for example). Widespread adoption of these prosumer-based products has not only led to an increase in the production of information, but also to the consumption thereof (Ritzer & Jurgenson, 2010). Importantly, such consumption is not a new concept. In fact, Jean Baudrillard had already coined the term *consumer society* in the 1970s (Baudrillard, 2016). Baudrillard's foresight in these matters is quite striking in that he was able to foresee the fundamental tenets of social media, decades before its creation. So accurate is his description of this phenomena that he specifically stated (Scott, 1983, p.17),

> *"You are the news, you are the social, the event is you, you are involved..."*

Using a famous 1970s television series about a family named *The Louds*, Baudrillard explicitly states that now there is only information. For Baudrillard, the medium has become entwined with the message in that they are now indistinguishable. As such, the singular panoptic source of information is,

> *"...diffused and diffracted..." (Scott, 1983, p.17)*

This takes place to such an extent that there is no means of providing society with a single distorted version of reality, since there are so many different versions thereof. Many of these ideas have direct parallels within the realm of social media. For example, the sharing of news and events covered by a variety of social media users, using a variety of mediums, often lead to a number of different interpretations of what actually happened. In some cases, there are so many interpretations that it is impossible to label one version as the definitive source of what we deem to be *real*. All these different interpretations produce more information which leads to more consumption (i.e., via Smart Phones, Desktops/Laptops, Smart Watches, and so forth). In fact, the levels of information consumption on social media is substantive, with a report by DOMO (2018) (a Big Data thinktank) reporting that for every minute:

- YouTube users watch 4,3 million user-generated videos,
- Twitter users send 473000 tweets,
- Instagram users post over 49380 photos,
- Google conducts 3,8 million searches,
- Facebook Messenger is used to send over 25000 GIFs (type of picture), and
- American citizens consume 3,1 Terabytes of Internet data.

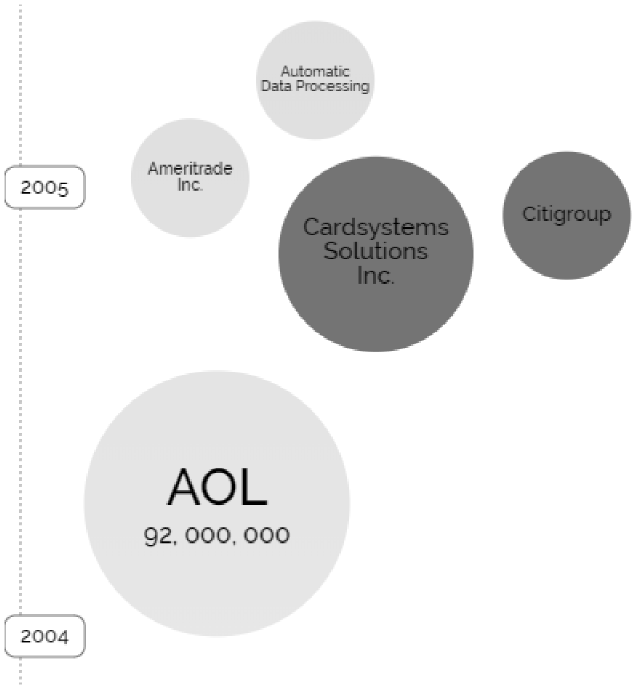


Figure 3.2: Data breaches circa 2004 (adapted from www.informationisbeautiful.net)

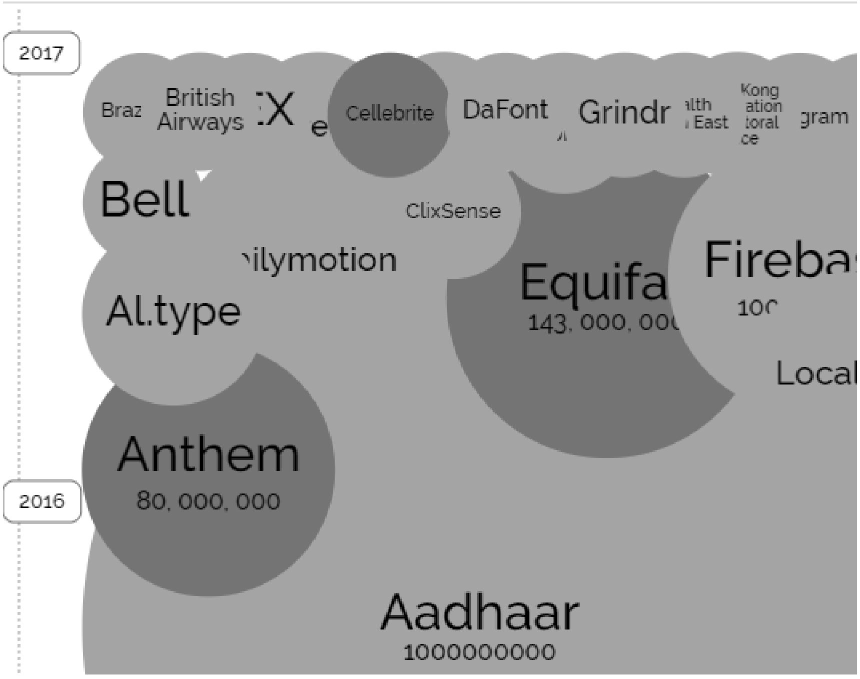


Figure 3.3: Data breaches circa 2017 (adapted from www.informationisbeautiful.net)

This abundance of social media-based information further fuels the information economy. More interactivity and socialisation options requires more clicks and thus, more data to be accumulated (Andrejevic, 2007, pp.2-7). Adding to these statistics, Figure 3.2 illustrates the number of data breaches that took place around the same time Facebook was created.

From this illustration, one can see that there were very few known information breaches. This stands in stark contrast to Figure 3.3, which illustrates data breaches in and around 2017. Thus, even the illegitimate (via data breaches) demand for information benefits from society's obsession with the consumption of thereof. In turn, this assists those social media corporates who make it their business to profit from the surveillance of social media-based data.

3.4.1.1 Surveillance of social media-based data

From these descriptive statistics, it is clear that a large amount of social media-based data exists on a variety of platforms. However, its existence does not necessarily constitute surveillance thereof. From the earlier definition and literature, there are primarily two reasons why the surveillance of data is performed, namely, investigating and monitoring. As such, there needs to be a reason for conducting the surveillance.

Fuchs & Trottier (2015) agree, adding that the reasons for conducting surveillance are also violent in nature, defining it as a trifecta consisting of physical, structural, and cultural dimensions. These different types of violence are then enacted, based on the reason for conducting social media surveillance. For example, if police use social media data to monitor content in order to prevent some future criminal act, they are making use of structural violence. Importantly, although there are a myriad of technical means to perform social media surveillance, the reasons are mostly (if not always) social in nature (Brown, 2015). Thus, social media surveillance can be defined as,

> *"...a techno-social process in which human actors make use of surveillance technologies for monitoring human activities on social media." (Fuchs & Trottier, 2015, p.127)*

In the years before mainstream social media (i.e., Facebook), the reasons for conducting surveillance of data were mainly related to the monitoring of society, as explained in Section 2.1. Although monitoring still takes place, social media itself has become an enabler. In an effort to amass more data, social media corporates try their best to entice users to participate and sign-up to their services by creating sign-up portals that are *plain*, and for the most part, *culturally agnostic* (van der Schyff et al., 2018). Together, the ubiquitous and pervasive nature of social media has enabled it to become a perfect platform to use if one wishes to investigate and monitor data, either as a corporate, a government, or an individual.

One such form of investigating is data mining. Data mining allows for the identification of patterns and relationships within large sets of data (often disparate) that would not have been visible otherwise. Here, it is the analysis of large datasets (with the intent to predict) that typifies the use of social media data. For example, Moro et al. (2016) made use of social media-based data mining to predict the impact of social media performance metrics on the process of brand building. In a similar article, Moro et al. (2014) used social media data mining to predict how successful banks' telemarketing efforts were likely to be. Authors have also used social media data (Twitter in particular) to predict market revenues (Asur & Huberman, 2010) or even earthquakes (Sakaki et al., 2010).

Importantly, data mining is algorithmic and technical in nature (Hajian et al., 2016). For example, Carah (2017) studied how consumer brands can be used as actors in experiments designed to refine algorithmic decision making. Carah (2017) specifically states that such social media-based algorithms not only facilitate the creation of categories, but it also allows them to target specific consumers. Similar investigative forms of data mining are conducted by companies who perform background checks on prospective employees, such as Social Intelligence[1].

Furthering this argument, it is clear from in-depth interviews with both Michael Hayden (former CIA director) and Edward Snowden (CIA whistle-blower) that several technology corporates (including Facebook) funnel data to the Central Intelligence Agency (CIA) for investigative purposes as part of the PRISM surveillance programme (Fuchs & Trottier, 2015; Hayden, 2014; Snowden, 2016). Importantly, this initially took place without the users being aware of it. Even the very nature of social media sharing has led to the creation of similar intelligence platforms that allow intelligence personnel to share investigative information across agencies. Examples include A-Space (analytic space), TAGConnect, and Intellipedia (Werbin, 2011).

Whereas investigative surveillance (for both intelligence and corporate reasons) makes use of social media-based data that already exists on the platform, location-based surveillance is used in a monitoring capacity. As such, these services are in part responsible for

[1] www.socialintel.com

the data that is generated and funnelled to the social media platform - typically from a mobile device (Lupton, 2012). In turn, because this data is directly related to the geographic behaviour of social media users, it enables social media corporates to perform behavioural analyses. For example, using data gathered via a mobile device's location sensors, it is possible not only to determine where a user is at any given time, but also to monitor their movement (Wilken, 2014).

Over and above merely monitoring the movement of users, location-based data can also be combined with other social media-based data. For example, Google Maps (a Google App) will, at times, prompt users to review a location, shop, or visit a restaurant simply because that user was in close proximity to those locations. Such reviews not only benefit the platform, but also the third parties with whom it is shared.

Other examples include using e-health Apps on mobile devices. It is somewhat ironic that users of e-health Apps do so primarily to monitor themselves. Depending on their need, this can range from the number of steps taken per day, the level of alcohol consumption, or merely monitoring their eating habits. In many instances, these Apps then allow for the results to be uploaded and shared via a social media profile. This again fuels information consumption, since other users are able to interpret and compare these results with their own. This data can then be mined and analysed (by the App developer) to determine behavioural patterns and matches across many other users of the same App. For example, Symeonidis et al. (2018) found that inadequate privacy settings as well as sub-optimum server communications, made it easy to retrieve personal information via third-party Facebook Apps. Using the AppInspect dataset, Symeonidis et al. (2018) demonstrate that App developers are able to extract data from one App, but also to 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. These results can then be used to improve the related product/App, but also to commodify it. Again, even though users of these Apps voluntarily provide their personal information and agree to upload their results, the use thereof beyond that is something they are not made aware of.

3.5 Facebook App surveillance

It is problematic that the mediums we rely on to communicate with (Smart Phones, Desktops, and Laptops) have become part of social media corporates' business model. Potential users of social media services are not permitted to participate and thus create their own version of Baudrillard's *real* unless they provide these services with their personal information. In and of itself, this is not a problem; however, once a user starts using the services, a surveillance process is initiated that monitors the behaviour of that user whilst using the service (Brown, 2015).

Even in this regard, some social media corporates, like Facebook, have made it possible for users to adjust what other users and friends can view on their profile. However, these privacy settings undergo frequent changes making their use problematic as the only means of curtailing the surveillance of their personal information (Shore & Steinman, 2015). Additionally, the privacy policies associated with these mechanisms are also frequently amended. As such, from an information security perspective, the state of a Facebook user's personal information is always in flux, making it difficult for the average user to know exactly how, when, and where their personal information is being used by Facebook.

One way in which Facebook collects and shares personal information is via the Apps available on the platform itself (i.e., through the App Center) or the many third-party Apps that use Facebook Connect. For example, Spotify makes it possible for the users of their App to sign in and use Spotify with their Facebook credentials. However, if a user elects to do this, Spotify receives the following personal information from the Spotify user's Facebook profile:

- Public profile,
- Friends list,
- Birthday, and
- Email address.

Although an individual can elect not to share their friends list, birthday, and email address, this requires several changes during the sign-in process. Importantly, users are not able to hide their public profile from Spotify, if they sign into the App using their Facebook credentials (i.e., it is mandatory). There are many other Apps that work in a similar manner. Candy Crush Saga and 8 Ball Pool (both top of the Facebook App Center charts) also receive similar information if you sign in with a Facebook account. Even certain Wi-Fi products can be remotely controlled by signing into the supplied third-party App with an individual's Facebook credentials; even if the device is located behind a firewall. However, users are not aware of the information security implications when using these Apps.

One prominent example of the misuse of personal information collected via an App is that of the Cambridge Analytica incident. Using an App called *thisismydigitallife* Aleksandr Kogan enticed users to take a personality quiz which required them to give the App access to the personal information on their Facebook profile (DigitalWatch, 2018). Although the 270000 users who installed and completed the personality quiz were aware that their information would be harvested, they were not aware that the App could also harvest the profile data of their Facebook friends; something the Facebook API allowed at the time. In turn, this allowed the App to harvest the personal information of over 50 million United States citizens (i.e., through users' network of friends). Of course, Kogan then violated his Facebook research agreement and sold the data to Cambridge Analytica, who subsequently used it to perform personality-based analyses of 30 million United States voters. The so-called *persuadables*.

Following the resultant public outcry and Zuckerberg's congressional testimony, Facebook set out to correct these issues and subsequently suspended over 400 Apps (circa September 2018) (Coldewey, 2018). However, this is only one dimension of the larger problem. Over and above the Facebook-authored Apps, Facebook also gave over 60 device manufacturers privileged access to their social media platforms, so as to build their own Facebook-integrated Apps (Leetaru, 2018). More concerning is the fact that some of these manufacturers have been flagged by the United States intelligence community as a threat to national security. Again, researchers openly state that although Facebook tries to console their users by creating more elaborate privacy settings they still,

> *"...fail to educate lawmakers and the public about the full extent of [the] access it provides to others of user data." (Leetaru, 2018)*

This continues in the aftermath of the Cambridge Analytica scandal. Additionally, it is also particularly problematic that Facebook seems to sidestep legislation by simply absorbing these third parties into their parent company, so as to claim that they are simply an extension of the parent company. However, given that modern society's demand for information has been steadily increasing since 2004, the acceptance or *soft sell* is becoming easier to justify, and thus users seem to overlook these problems. For users, it is far more enticing to participate on Facebook, which allows them to create their own version of reality. As such, acceptance without considering the consequences seems to be the norm.

So, even though there are a number of issues relating to how Facebook utilises their users' personal information, many users continue to use the platform. To some extent, this is understandable, given how dependent society has become with regards to the use of technology as well as the resultant demand and consumption of information.

3.6 Summary

This chapter covered a number of critical aspects that either attribute to or are directly responsible for the more significant problem this thesis aims to address, namely, the surveillance of Facebook-based personal information. From the historical overview it is clear that the surveillance of data has indeed come a long way and although it was initially conducted to combat fraud and aid efficiency, ultimately governments and corporations have used it as a means to increase societal control and capital. Harnessing an individual's need to build and maintain social relations with others, corporations (like Facebook) have made it their goal to capitalise on both their users' online behaviour and personal information. In turn, this has led to the exploitation of these users, by turning their online existence into a commercial endeavour.

Although recent research has been conducted on the concept of information security awareness when using Facebook Apps (Symeonidis et al., 2018), it ignores the psychological aspects thereof. On the other hand, those studies that include psychological aspects, including personality traits, do so by focusing on general Facebook use and thus fail to explore Facebook Apps specifically (Amichai-Hamburger & Vinitzky, 2010; Eşkisu et al., 2017; Koban et al., 2018).

This study aims to investigate this by exploring how the personality traits of a Facebook user influences their information security awareness of the surveillance conducted via Facebook Apps. As one component of the latter investigation, the following chapter presents a review of not only personality traits, but also how they have been used in similar behavioural information security research.

Chapter 4

INFLUENCE OF PERSONALITY

"Success consists of going from failure to failure without loss of enthusiasm."

— Winston Churchill

The previous chapter discussed the surveillance of data by making use of concepts such as consumerism and prosumerism; arguing that the increased demand for information has made social media a lucrative milieu within which to perform such surveillance. Additionally, Chapter 3 alludes to the fact that social media has made it easier for users to access this information. Importantly, users' psychological and social needs act as the primary catalyst to engage with social media. This chapter aims to elaborate on these psychological aspects, by discussing how personality influences an individual - specifically at the behavioural level. The chapter presents the reader with a broad overview of personality theory and then discusses trait theory; more specifically the Big Five. The rest of the chapter motivates the use of the Big Five, illustrates how personality theory aligns with the Theory of Planned Behaviour (TPB), and concludes by reviewing other studies that have also investigated the behavioural influence of an individual's personality.

4.1 Personality theory in perspective

An individual's personality is viewed as a set of aspects that determines how they feel, make sense of the world, and ultimately behave (Lane & Manner, 2011). It is said to be stable across the entire lifespan of an individual and cannot be modified by direct intervention (Warkentin et al., 2012). In fact, Cattell believed it to be impossible to change an individual's personality (Schultz & Schultz, 2016, p.214). Generally accepted as a concept with diverse means of measurement, psychologists have only recently agreed on the fundamental traits that comprise an individuals' personality, which Schultz & Schultz (2016, p.6) defining it as,

> *"The unique, relatively enduring internal and external aspects of a person's character that influence behaviour in different situations."*

Having said this, the resultant *agreed upon* models are for the most part, based on a number of personality theories. Some of these theories vary considerably, depending on the theoretical approach and assessment methods used (Heinze & Hu, 2007). For example, Schultz & Schultz (2016) outlines nine different categories of personality theories. Although this study uses a trait-centric approach, it is interesting to note that these authors do not strictly consider it to be behavioural in nature.

Referred to as behaviourism, psychologists like John Watson, opposed the idea that it is worth studying the unconscious. For these psychologists, it was far better instead, to study behavioural responses to a selected external stimulus - thus favouring a more objective stance to experimentation. Conversely, Sigmund Freud found no use for experimentation and only made use of patient interview data in his psychoanalytic analyses, which typified early personality-based research.

Although psychology initially ignored the role of personalities, it was through the work of Murray, Cattell, and Allport that it started to appear in American psychology (circa 1930s). Allport and Cattell advocated the trait-centric approach, which has been used as early as 460 B.C. by the Greek physician Hippocrates - albeit in a more straightforward form. For example, Hippocrates grouped individuals into four categories: happy, unhappy, temperamental, and apathetic (Schultz & Schultz, 2016, p.191). For Hippocrates, membership was determined by an individual's biological make-up. As such, he dismissed the influence of cognition and experience. Because these trait theorists viewed personality as something biological, they received much criticism. After all, if an individual's personality is comprised of predetermined traits, then similar personalities should behave similarly. Of course, experimentalists such as Skinner and Bandura would disagree, stating that there are other factors that influence behaviour - specifically those factors situational and environmental in nature.

In this regard, the work of Allport and Cattell is somewhat misunderstood. Although they emphasised the role of biology, they also acknowledged the behavioural influence of an individual's environment (Pervin & John, 1997, p.250). It is this balanced approach to the study of personality that has become not only popular, but also vital in modernity. Unlike the psychoanalytic approaches, which derived theory from the study of psychologically unstable individuals, their approach focused on the use of emotionally stable individuals from all walks of life - a more representative sample as such. Importantly, Allport considered personality traits to not only influence behaviour, but also that they differ depending on the situation.

In this study, these behavioural aspects are essential, considering that its objective is to theorise the behavioural influence of personality. This includes the influence of social norms, which could be understood to resemble different situations or environments. For example, if a Facebook user finds him or herself in a familial environment where the use of Facebook Apps is taboo, they may elect not to use them. The opposite may be true in a situation where the same individual is surrounded by friends.

4.2 Trait-centric approaches

There are a number of proponents of a trait-centric approach to personality theory; most notably, Allport, Cattell, Eysenck, McCrae, Costa, Buss, and Plomin. Although they have different perspectives on how personality influences behaviour, there are a number of similarities which are still published in modern personality psychology textbooks.

4.2.1 Personality traits

According to Allport, traits are comprised of several habits and differ significantly from one individual to the next. Together these traits guide an individual's behaviour, subject to the influence of social, environmental, and cultural factors. In this way, Allport's personality theory states explicitly that an individual's personality is comprised of traits unique to that individual (personal dispositions) as well as those that are shared with others.

Personal dispositions are then further divided into three categories depending on the intensity of the trait in question. If a trait is particularly dominant, it is referred to as a cardinal trait (Schultz & Schultz, 2016, p.198). In contrast, central traits are especially important when considering the influence personality may have on behaviour (between five and ten were identified by Allport). The remaining traits are then labelled as secondary, as they are exhibited inconsistently (Pervin & John, 1997, pp.228-232)

In contrast, Cattell's theory does not directly address habits. In fact, Cattell completely integrates his view of motivation with that of the traits his theory advocates. Like Allport, Cattell also distinguishes between traits common to a larger set of individuals (a common trait) and those unique to each individual (unique traits) (Cervone & Pervin, 2014, p.243-244). These act as an overarching means of categorising traits. However, Cattell also provided a second means of categorising traits. In the the latter organisation scheme, a trait is either categorised as an ability (describe skills), temperament (behavioural style), dynamic or surface trait (Pervin & John, 1997, pp.244-245). Although Cattell regards dynamic traits - those that describe motivations - as important, he also frequently referred to source and surface traits. These latter traits have become the core building blocks of his trait-centric approach.

Together with surface traits, source traits are considered to be stable and permanent. Using an assumption referred to as the *lexical hypothesis* Cattell identified 16 source traits (Chamorro-Premuzic, 2016, p.50). These 16 traits are similar to those found in the Five-Factor model of McCrae and Costa, but are represented in bipolar form when assessed. Within these, Cattell further distinguishes between constitutional and environmental traits. For example, certain biological situations lead to behaviour that is only exhibited under those specific conditions. Slurred speech is one such behaviour exhibited when an individual is drunk. Those traits, environmental in nature are learned from one's physical and social sphere and are referred to as sentiments (Schultz & Schultz, 2004, p.280).

An individual's attitudes towards their wife, religion, or Facebook can thus be regarded as sentiments. Importantly, for Cattell both sentiments and ergs (meaning work or energy) drive all behaviour. Considered to be constitutional in nature Schultz & Schultz (2004, p.279) list several examples of ergs including anger, appeal, and curiosity. Unlike sentiments, which are learned, ergs are permanent personality structures - they may lessen to some extent, but never disappear. For example, an individual may enjoy using Facebook Apps out of curiosity and then start using it less due to anger and frustration (possibly related to surveillance), but as this anger subsides the individual may start using it again as frequently as before. As such, the ergs are still present, but just to a different degree.

The role of sentiments is thus a vital part of how individuals' attitudes are shaped. This is especially pertinent if one considers that Cattell regards it as something that is learned. Consider the latter Facebook App user. Here, their anger (related to surveillance) could be viewed as a consequence of them learning about (or being made aware of) such forms of surveillance. In turn, their level of anger increases, resulting in a behavioural change (i.e., they are using the Facebook App less, more carefully, or not at all).

4.2.1.1 A genetic perspective

Although both Allport and Cattell acknowledged the possibility that genetics could influence personality, it was psychologists such as Eysenck that actively researched this relationship. Often referred to as behavioural genetics, Eysenck pioneered this form of personality research, resulting in the creation of several assessment instruments and hundreds of publications (over 700). Like Cattell, he also used factor analysis, but not exclusively. For example, Eysenck also used other personality tests and experiments, attributing much of his success in developing these research tests and questionnaires to his wife. Essentially Eysenck's theory is based on three personality dimensions (referred to as the Gigantic Three), each comprising several trait combinations. These dimensions include:

- Extraversion as opposed to introversion.
- Neuroticism as opposed to being emotionally stable, and
- Psychoticism as opposed to being able to control impulses.

For example, being sociable, active, assertive, and carefree are all traits Eysenck's theory classifies under the first category listed above. Importantly, research has shown that these dimensions are stable and stay with an individual throughout their life. This bears some similarity with the ergs described by Cattell, since just as the dimensions (ergs) are always present, it is only the intensity that changes depending on situational or environmental factors. However, there are some significant differences with other trait theorists.

For example, Eysenck's research found that introverts possess lower levels of cortical arousal, which necessitates them seeking outside stimulation. Conversely, introverts have higher levels of cortical arousal and thus requires less stimulation (Schultz & Schultz, 2004, p.290). Eysenck also found that individuals high in Neuroticism display more brain activity in areas of the brain that regulate sympathy within the autonomic nervous system. This includes functions such as breathing and blood flow. In neurotics, this system overreacts to environmental stress elements, which increases sensitivity.

This is not found in extroverts, for example (Cervone & Pervin, 2014, p.255). For Eysenck even Psychoticism showed some relation with genetics. Because many of the traits associated with Psychoticism (including aggression, egocentrism and impulsiveness) are more pronounced within men, Eysenck's research implied that this could be attributed to male hormones (Schultz & Schultz, 2016, p.291).

4.2.1.2 HEXACO and the Dark Triad

Similarly, Arnold Buss and Robert Plomin also identify three personality factors, but do so by further subdividing Cattell's temperament personality trait. Thus, Buss and Plomin identify traits such as emotionality, activity, and sociability, which together determine if an individual is an extrovert or introvert. These are then regarded as supertraits (Schultz & Schultz, 2004, p.298).

In recent years two new trait-centric approaches have been proposed namely, HEXACO and the Dark Triad. At first glance, one might mistake HEXACO for the Big Five, since it consists of six traits of which four share lexical descriptions with those of the Big Five. However, upon closer inspection, it becomes clear that only Conscientiousness and Extraversion are similar in composition, with the other traits differing to a larger extent. For example, instead of Neuroticism, the HEXACO model makes use of a trait called Emotionality with the sixth trait being defined as Honesty/Humility (Schultz & Schultz, 2016, p.239).

In contrast, the Dark Triad is comprised of three personality traits that not only differ lexically, but also in the way they are portrayed. For example, most of the other personality models' traits are not fundamentally negative when considering the individual differences they are comprised of. This is not the case with the Dark Triad, which consists of three traits, namely, Machiavellianism, Psychopathy, and Narcissism. It is thus clear that the Dark Triad was created to explore the darker aspects of an individual's personality. As such, it is not uncommon to see the Dark Triad employed to explore the behavioural influence within areas such as cyberbullying, addiction, dependencies, office politics, and mental disorders (Goodboy & Martin, 2015; Kardum et al., 2017; Kircaburun et al., 2018).

4.2.1.3 The Big Five

Unlike Eysenck's focus on behavioural genetics, Paul Costa and Robert McCrae also relied on factor-analytics to derive their personality traits inductively (Burger, 2018, p.144). Because their model is comprised of five personality traits, it is commonly referred to as the Big Five (Burger, 2018, pp.142-144). Using a variety of assessment methods, Costa and McCrae's personality traits find some overlap with that of Eysenck in that they also acknowledge the existence of Extraversion and Neuroticism. However, instead of Psychoticism they also identified Openness (sometimes referred to as Openness to Experience), Agreeableness and Conscientiousness.

Individuals high in Extraversion are generally sociable, energetic, positive, seek excitement and are known to engage in risky behaviour (Amichai-Hamburger & Ben-Artzi, 2003; Karim et al., 2009; Winter et al., 2014; Giluk & Postlethwaite, 2015). They also prefer to work within a team and generally have more friends and romantic relationships of a higher quality (Warkentin et al., 2012; Seidman, 2013). These individuals also tend to represent themselves strategically and are self-conscious. Interestingly, although individuals high in Extraversion tend to like others, they are not necessarily likeable (James et al., 2017). Additionally, those high in Extraversion are more likely to display behaviour in line with their perception of how significant others think they should behave (Devaraj et al., 2008). As such, it is plausible that individuals high in Extraversion are more likely to make use of Facebook Apps, if significant others are also using Facebook Apps. Conversely, individuals low in Extraversion tend to be lonely and reserved individuals who prefer a passive approach to life (Bashir et al., 2017).

Neuroticism typifies individuals who tend to be emotionally unstable, nervous, depressed, and experience high levels of frustration (De Feyter et al., 2012; James et al., 2017). As such, these individuals are emotionally charged, anxious, sensitive, impulsive, and tend to worry (Hughes et al., 2012; Gohary & Hanzaee, 2014; Pentina et al., 2016). They also exhibit a negative attitude towards both work and life in general, which shapes their perception of the usefulness of technology. These individuals find technological change stressful and do not regard changes in a positive light. This stems mainly from the fact that it may require others to investigate actively and understand how they work (i.e., thus being monitored or surveilled), which make these individuals distrustful of technology and others (Devaraj et al., 2008; Lane & Manner, 2011). This is especially important if one considers that individuals high in Neuroticism tend to use the Internet for selfish reasons, without thinking how their behaviour might affect others (Karim et al., 2009). This negativity affects not only their life, but also their ability to form meaningful relationships.

In turn, this makes them lonely individuals (Amichai-Hamburger & Ben-Artzi, 2003). Moreover, because individuals high in Neuroticism fear embarrassment, have low self-esteem, are insecure (thus seeking reassurance from others) and suggestible, it is likely that they also place great emphasis on how significant others think they should behave (Zhang, 2006; Bansal et al., 2010; Koban et al., 2018). It thus stands to reason that individuals high in Neuroticism are more cautious when sharing personal information via Facebook Apps. One extreme being that they completely avoid the use of Facebook Apps (Skues et al., 2012). In contrast, those individuals low in Neuroticism are emotionally stable, have a positive outlook on life, and are socially healthy (Bashir et al., 2017). Such individuals tend to be ethical, possess values, and are less likely to abuse the Internet (Karim et al., 2009).

Individuals high in Openness to Experience (also referred to as Openness) are intellectually curious and tend to enjoy (and pursue) new experiences (Skues et al., 2012; Moore & McElroy, 2012). Such experiences may include the exploration of new and varied technologies (i.e., Facebook Apps for example) (Zhang, 2006; Xu et al., 2016) and since these individuals are usually creative, motivated and imaginative, Openness is often correlated with higher cognitive abilities (Lane & Manner, 2011; Moore & McElroy, 2012; Xu et al., 2016) as well as leadership emergence and effectiveness (Chamorro-Premuzic, 2016, p.350). Additionally, individuals high in Openness are flexible from a behavioural perspective and possess an innate tolerance for that which is new - especially occupation-based technology and choices (Costa Jr & McCrae, 1992; Devaraj et al., 2008; Lane & Manner, 2011; Gohary & Hanzaee, 2014). They also tend not to judge and generally avoid conforming to accepted norms, which makes it less likely for these individuals to place an emphasis on how significant others think they should behave (Warkentin et al., 2012; Pentina et al., 2016). Individuals high in Openness (but low in Agreeableness, Conscientiousness, and Neuroticism) may also display a greater inclination to engage in risky behaviour (McCormac et al., 2017). Additionally, individuals high in Openness to Experience display a general disregard for authority, which may conflict with individuals high in Extraversion who exhibit strong correlations with assertiveness and the ability to lead (Chamorro-Premuzic, 2016, p.73) — for example, making use of new (possibly untested) Facebook Apps. Conversely, individuals low in Openness to Experience are more conservative, avoid uncertainty, and abhor any form of change (Hughes et al., 2012). As such, they are more likely to conform and support the status quo.

Individuals high in Agreeableness are somewhat self-conscious and are generally concerned with what others think of their behaviour (McCormac et al., 2017). They also tend to volunteer, perform community work, and exhibit a tendency to be concerned for others' well-being (Chamorro-Premuzic, 2016, p.72). As such, Agreeableness is highly predictive within environments where individuals need to help, cooperate, and nurture others (Barrick et al., 2001). They thus tend to be friendly, trusting, and respect the beliefs of others (Giluk & Postlethwaite, 2015). Furthermore, they also portray a sense of optimism, leading them to assume that other individuals are also trustworthy and honest. Interestingly, much of the behavioural aspects attributed to Agreeableness are driven by fear (Karim et al., 2009). It is thus not uncommon to find that those individuals most likely to comply with organisational policies (such as information security policies) are high in Agreeableness. This is not surprising, since agreeable individuals are generally eager to comply with and adopt safety measures within the workplace because they fear sanctioned action (or even prosecution).

Conscientious individuals are organised, responsible and performance driven (Ross et al., 2009; Shropshire et al., 2015). They also tend to be thorough in everything they do, and like those high in Agreeableness exhibit strong tendencies to comply with information security policies (Hughes et al., 2012; Warkentin et al., 2012). Additionally, because these individuals pursue success, they are self-disciplined and persistent, which makes them successful in the workplace (Xu et al., 2016). Interestingly, it has been suggested that success in the workplace has a stronger relationship with Conscientiousness than emotional stability. This means that it is possible for at least some conscientious individuals to be somewhat unstable emotionally (Barrick et al., 2001). Additionally, individuals high in Conscientiousness tend to be reluctant online users who are cautious about the personal information they disclose (Ross et al., 2009). However, when these individuals do disclose information (on Facebook, for example) they do so to find and build social relations of a high quality (Seidman, 2013). This form of self-disclosure is performed by using as few features (of the social media platform) as possible and coincide with a propensity to upload less personal information (Koban et al., 2018). They also view social media activities as a distraction - something that detracts from their pursuit of achievement and success; especially within the workplace (Devaraj et al., 2008). In fact, according to Barrick & Mount (1991) it would difficult to find a job where such individuals would not be successful.

To some extent, this is further enabled by their planned and goal-oriented approach to their behavioural demeanour. In turn, this makes individuals high in Conscientiousness the least impulsive of all the personality traits within the Big Five. Like those high in Agreeableness, these individuals also follow accepted norms, are less accident-prone, and abide by the rules (Shropshire et al., 2015). From the evident presented above, it is thus likely that individuals high in Conscientiousness will avoid or make less use of Facebook Apps (i.e., viewed as a distraction). Moreover, any Facebook App that they do use will most likely be thoroughly investigated and require as little personal information as is necessary to function. Such cautious, deeply processed, and controlled behaviour is further fuelled by a dutiful sense of responsibility (Ross et al., 2009; Komarraju et al., 2011). Thus, when a conscientious individual decides to make use of a Facebook App, they will most likely do so in a responsible manner. Although the use of a few Facebook features, such as the privacy settings, contradict the findings of Koban et al. (2018) it may be likely that, of all the Facebook features available, they mostly use the privacy settings.

4.2.2 The applicability of the Big Five

Although the trait-centric approach in general (and the Big Five in particular) is popular, it is often criticised on a variety of fronts. Firstly, researchers debate what the five traits actually mean. If they are simply derived from the English language (similar to what Cattell did) are they not just merely linguistic constructs? From this one could deduce that the English language may not be adequately equipped to express all the nuances of an individual's personality (i.e., there may be some specific traits which simply can't be expressed). Having said this, researchers have done Big Five-based research in other languages and still found support for these five traits.

Coincidentally other researchers found support for the existence of up to seven and as little as one personality trait. However, this stems from some confusion on the trait of data to be used in the factor analyses. For example, it has been found that if evaluative traits are included, additional traits are identified. Additionally, when it comes to the interpretation of different research findings, it is important to understand how broadly personality has been defined within those studies. For example, if a broad stance is taken, findings may suggest a number of traits be classified under only one larger trait. However, if the same or similar studies were to adopt a narrow stance on personality, the findings may all be classified under specific traits. As such, it is not uncommon for findings who used the Big Five to seemingly contradict each other when in actual fact, they were simply based on different understandings thereof.

Issues regarding the stability of the traits have also been raised, with at least some evidence to suggest that Conscientiousness and Agreeableness increase with age. This raises more issues concerning how specific researchers should be when creating a research outline, in order to account for such findings. In fact, it is generally accepted that it is better to use a specific instrument if one wishes to evaluate a specific personality trait. As such, the Big Five is useful to give a researcher a broad understanding of all possibilities, but it is likely to be less effective if a study only wishes to focus on specific individual difference that is usually associated with a trait. For example, if a researcher wishes to study only information security policy compliance, it may be better to only focus on instruments that evaluate Conscientiousness and Agreeableness, or even individual traits that constitute each one. In this manner, the researcher obtains a more accurate understanding of the problem. Of course, this depends on the problem at hand, as well as the desired perspective. If the study breaks new ground, it may be beneficial to first get an overview using all the Big Five traits after which further research could delve into specifics.

Nevertheless, a trait-centric approach can provide much behavioural insight, and has been in development since 1936 (Shropshire et al., 2006). For example, if traits had no behavioural influence, organisations would have no statistical means of selecting employees or in the very least building dynamic and balanced teams. In fact, if trait-centric research were invalid, it would make no sense to perform any trait-centric screening, since an individual's behaviour would change from one situation to the next (i.e., there would be no means to predict behaviour). There are also historical reasons to reconsider the reliability and validity of trait-centric approaches. For the most part, this relates to the instruments used at the time when trait-centrism was relatively new (circa 1960s). Often these instruments consisted of just one item! For example, the personality instrument (BFI) used in this study consists of forty-four items with a number of studies that attest to its reliability and validity across a broad range of topics, demographics and cultures (Gosling et al., 2003; Srivastava et al., 2003).

Other instruments, such as the Myers-Briggs Trait Indicator (MBTI) comes in various forms ranging from 93 to 222 items and is commonly used by recruitment agents and employers alike. Over and above reliability and validity issues, some pro-situational researchers do not agree that accounting for 10% of the variance is significant. To investigate this, further research was conducted to find out just how statistically significant other situational findings are. According to Burger (2018, p.152) it was found that these so-called *landmark* findings displayed correlation coefficients ranging from 0.36 to 0.42, which trait-centric studies deem to be weak at best. Burger (2018, p.153) provides more evidence in favour of a trait-centric approach stating that some studies (measuring cognitive ability for example) are unable to account for as much of the variance as personality traits. It has thus become not only common, but also acceptable for trait-centric approaches to account for only a portion of the variance - especially since Burger (2018, p.153) states that,

> *"When trying to predict behaviour from personality test scores, we must remember that most of the behaviours we are interested in are determined by a large number of causes."*

Additionally, the Big Five also allows for comprehensive comparison of findings (Chamorro-Premuzic, 2016, p.57). Furthermore, because the traits are lexical in nature, it is possible to map most findings of other studies to one or more of the traits within the Big Five - hence its widespread use in not only clinical psychology, but also applied psychology (Costa Jr & McCrae, 1992; Barrick et al., 2001). Such uses stem from a general consensus that the Big Five can be used to illustrate:

- Its universality and dominance amongst other trait-centric models (Vassend & Skrondal, 2011; Eşkisu et al., 2017),
- Trait consistency across the life-span of individuals (Costa Jr & McCrae, 1992), and
- Its use within the context of several theoretical frameworks, methods of assessment, cultures, as well as gender (Costa Jr & McCrae, 1992; Ryan & Xenos, 2011; Seidman, 2013).

Even analyses using different scales confirmed the existence of only five traits for both men and women. Moreover, some of these scales were even translated yet still produced only five traits (Costa Jr & McCrae, 1992). The Big Five has thus emerged as a model that is often used to understand the systematic behavioural influence of the individual differences that comprise the five traits (Devaraj et al., 2008; Komarraju et al., 2011). Importantly, it is regarded as a better personality model when dealing with technological issues, as opposed to other models (i.e., MBTI, for example) (Lane & Manner, 2011).

4.3 Behavioural influence in perspective

There are a number of studies that attest to the behavioural influence of personality. For example, in a study on Facebook addiction Marino et al. (2016) found that individuals high in Conscientiousness to be vulnerable in this regard. Such individuals strive for improvement and order, which may cause prolonged use to increase their number of friends and organise content. Interestingly, it is precisely this fixation on being structured, prepared, and composed that leads highly conscientious individuals to display problematic behaviour. Structure is used to order content, and more friends are added. More content is accessible and ultimately created, which necessitates more re-structuring - so the cycle continues leading to problematic Facebook behaviour.

Dependencies among highly neurotic individuals is also quite commonplace. For example, low levels of emotional stability and loneliness, especially amongst women and younger individuals in general, often lead to the increased use of not only Facebook (Hughes et al., 2012), but also the Internet as a whole (Amichai-Hamburger & Ben-Artzi, 2003). These individuals need to control information, but more importantly, they need to feel a sense of belonging and thus often behave impulsively (Gohary & Hanzaee, 2014). Note that these individuals are not lonely because they use the Internet, but rather attracted to this behaviour out of an existing sense of loneliness. This is not necessarily the case for adults over the age of 30 who also happen to be emotionally unstable. These individuals, conversely, are less likely to use social media (Correa et al., 2010). Unlike Amichai-Hamburger & Ben-Artzi (2003), other researchers, such as Tuten & Bosnjak (2001) only found evidence of increased Internet use among individuals high in Neuroticism and not also social media. This is important, since it furthers the argument that personality exerts a behavioural influence in general - albeit in response to different environmental and situational factors.

The aforementioned are likely also to influence the use of Facebook Apps. Consider the use of Spotify (a music streaming App) by a highly neurotic Facebook user who has logged on to the App with their Facebook credentials. The user is 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 music play-lists. Being aware that their personal information is accessible by Facebook may not be an issue, since theory suggest that the aforementioned sense of belonging, and need for self-validation are core individual differences within Neuroticism.

With a desire to constantly keep in touch with a myriad of friends (usually made offline) and a need for stimulation (i.e., cortical arousal) individuals high in Extraversion may also find social media platforms (such as Facebook) particularly appealing (Wilson et al., 2010). Because these traits classify individuals based on levels within each trait, it is possible that these individuals only exhibit such behaviour when they are also high in Neuroticism - hence the need for continued Facebook use.

Although this study's research instrument does not address the types of Facebook Apps used, it is plausible that these have at least some influence on the intended use within the context of Facebook Apps in general. For example, several Facebook Apps, specifically those in the App Center, are games or at the very least leisure-oriented Apps. This introduces additional dimensions, such as competitiveness, gratification, and even greed, to the extent that some Apps allow users to accumulate credits with which to purchase/unlock additional content. For example, when individuals low in Extraversion play games online, they actively try and exude a sense of confidence, which is usually only found among individuals high in Extraversion (Codish & Ravid, 2014).

Notwithstanding such forms of gratification, not all forms of gamification results in a perceived influence on playability. For example, research has found that the use of leaderboards is universally disliked and is perceived as a demotivating factor for not only individuals low in Conscientiousness, but also those low in Extraversion (Correa et al., 2010). This contradicts the findings of Codish & Ravid (2014). This should be even more of an impediment when using Facebook, since users are forced to make use of real names and email addresses (i.e., these details are vetted). It is thus likely that individuals high in Conscientiousness will avoid making use of similar Facebook Apps. When one considers the theoretical tenets of highly conscientious individuals, there are some contradictions here. For example, trait theory suggests that individuals high in Conscientiousness generally avoid social media, since it is viewed as a distraction. Given that games in general are goal-oriented, these theoretical tenets require more detail and it is possible that a conscientious individual's definition of a goal is very different from that which is generally accepted. Possibly these goals need to be qualified as a goal towards something that is not a function of self-interest (as is the case with gaming). Codish & Ravid (2014) do not elaborate on the combination of traits possessed by the conscientious individuals in their study, and it is thus plausible that many of these individuals were also high in Agreeableness. As such, they most likely also viewed leaderboards as something that might psychologically impede (or even harm) other players. Interestingly, individuals low in Extraversion enjoyed the inclusion of rewards, which is indicative of competitiveness. It is thus likely that gamified Facebook Apps will find resonance with these individuals as long as the App allows the use of nicknames, as opposed to the real name of the Facebook user.

Other studies which evaluated the use of Smart Phones, indicated that individuals high in Extraversion are more likely to own and use such devices. This corroborates known personality theory, which states that these individuals have a desire to communicate (Wolfradt & Doll, 2001). This includes the communication structures required to predict success within entrepreneurial behaviour (Leutner et al., 2014). It stands to reason that these individuals are likely to use Facebook Apps that facilitate such forms of communication. However, findings do suggest that individuals high in Extraversion are less likely to be involved in any creative entrepreneurial behaviour, since such behaviour requires an element of solitude (Leutner et al., 2014). Conversely, individuals high in Agreeableness were found to be more likely to phone other individuals and thus avoided indirect forms of socialisation, such as texting. Known theory suggests that individuals high in Agreeableness favour interpersonal relations, lending credence to the latter statement. It is thus unlikely that these individuals will make use of Facebook Apps that focuses solely on communicative actions. That being said, theory also suggests that individuals high Agreeableness are influenced by social (specifically subjective) norms and are deeply concerned about the security of their information (Shropshire et al., 2015). As such, intended behaviour towards continued use most likely depends on one's level of Agreeableness - something not explicitly stated in the study conducted by Lane & Manner (2011).

Personality also influences an individual's attitude. For example, authors such as (Shropshire et al., 2006, 2015), report the use of Conscientiousness and Agreeableness to ascertain individuals' intention to adopt security software. Here, Conscientiousness was found to be pivotal when analysing the behavioural influence of personality. Lane & Manner (2011) provides further evidence of the relationship between personality and attitude, stating that individuals high in Openness to Experience exhibit a positive attitude towards new technologies. However, when they do possess negative attitudes towards an intended behaviour they tend to be stronger than those of individuals low in Openness to Experience. As such, negative attitudes are likely to have a pronounced effect on the attitudes these individuals display toward the use of Facebook Apps.

Although authors, such as Bulgurcu et al. (2010), allude to the fact that information security awareness influences individuals' behavioural beliefs, they fail to address specific personality-based antecedents that influence awareness. Since awareness is not usually part of the TPB, substituting it for Perceived Behavioural Control (PBC) warrants some explanation. Theoretically, PBC is defined as the relative ease of performing a specific behaviour. As such, it is considered to be a significant predictor of behavioural intent (Jiang et al., 2016). One might ask which information or factors individuals rely on when making such an assessment?

This study argues that one such means of attaining the information is by educating individuals about the risks of disclosing personal information on Facebook Apps. From the analysis performed by Siponen (2001) it is precisely this lack of expertise that affects security-unaware individuals. It is thus possible that an educated individual - specifically focused on cybersecurity - will find it easier to effectively manage and make decisions related to the security of their personal information. Even knowledge acquired from one's circle of influence could sufficiently educate an individual and thus increase self-efficacy (Heinze & Hu, 2007). Given that extant research suggest that anxiousness influences an individual's motivation to act on their level of self-efficacy, one could posit that individuals high in Neuroticism will most likely perceive themselves as ineffective at managing the security of their personal information (Peleg et al., 2017). This may make them rely more on the default security settings when making use of Facebook Apps, since any changes made by themselves might be perceived as incorrect or insecure.

Conversely, confident individuals (like those high in Extraversion) are most likely to perceive the ease of securing their personal information as a trivial matter. However, this does not necessarily imply that these individuals are aware of the misuse of personal information when using Apps. If the central tenet of awareness within this context is education, it might be beneficial also to consider academic performance (i.e., appetite for learning). For example, De Feyter et al. (2012) found that Agreeableness and Neuroticism had a positive influence on academic performance. Given that these individuals place a strong emphasis on what others think, and that learning as a replacement of PBC increases awareness, it is plausible that individuals high in both Neuroticism and Agreeableness will exhibit higher levels of security awareness. In fact, overall De Feyter et al. (2012) found that personality traits had significant predictive power when determining academic performance.

Certain demographic factors also reveal interesting relationships when combined with the behavioural influence of an individual's personality. For example, studies have found a significant relationship between social media use and privacy disclosing behaviour among younger extroverts; especially females who also possess high levels of Openness to Experience (Correa et al., 2010; Hughes et al., 2012; Hollenbaugh & Ferris, 2014; Li et al., 2015). This is not the case with males, who share less and more shallow personal information. According to Cobb-Clark & Schurer (2012) this relationship is unlikely to change due to age, since most of the Big Five traits undergo changes independent of age. Zhang (2006) corroborates this finding, adding that females are generally higher in Conscientiousness and Agreeableness than men.

Like most individuals low in Extraversion, older individuals tend to use social media platforms that offer the ability to engage at both a cognitive and anonymous level. However, according to Bergström (2015), there is no gender difference when considering privacy concerns. In this case, one has to consider the context of Bergström (2015)'s study, which investigated privacy concerns across a broad range of uses. This reasoning is somewhat problematic, since females were found to be more concerned about the use of online debit card purchases. This contradicts their finding that there are no gender differences, but confirms the findings reported in Jeong & Kim (2017). It thus stands to reason that young females who are high in Extraversion and Openness to Experience are likely to make use of Facebook Apps. For example, if the continued use thereof requires online payments, they may be discouraged or concerned in the very least. However, if these Apps do not require any form of payment (as many do), it is likely that they will be open to disclosing personal information. Demographic factors (specifically gender) also have the potential to predict an individual's involvement with an online community, such as Facebook. For example, Chen et al. (2016) found the subjective influence on men to be particularly pronounced, whereas women were mostly unaffected. This stands in contrast to social role theory, which suggests that men are agentic and woman are communal (Chakraborty et al., 2013).

Although this study did not relate the findings to specific personality traits, it stands to reason that females are less likely to engage in the use of the Internet, social media or Facebook Apps based mostly on what significant others think they should do. Here, emotions (like loneliness) and associated motivations seem to play a cardinal role with some, albeit slight, variations when considering the behavioural influence of personality (see Figure 4.1 for a summary in this regard).

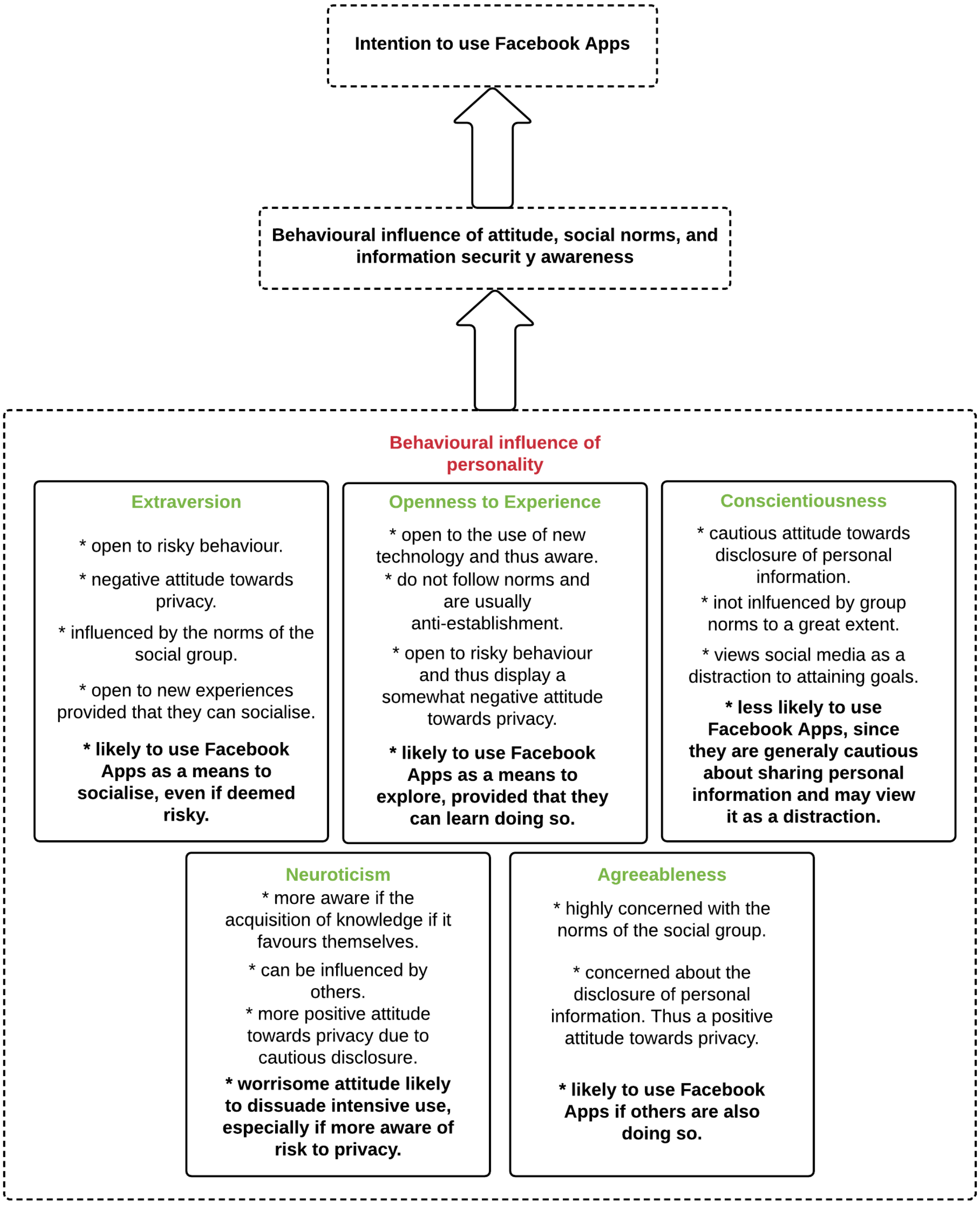

Intention to use Facebook Apps
Behavioural influence of attitude, social norms, and information securit y awareness
Behavioural influence of personality
Extraversion
* open to risky behaviour.
* negative attitude towards privacy.
* influenced by the norms of the social group.
* open to new experiences provided that they can socialise.
* likely to use Facebook Apps as a means to socialise, even if deemed risky.
Openness to Experience
* open to the use of new technology and thus aware.
* do not follow norms and are usually anti-establishment.
* open to risky behaviour and thus display a somewhat negative attitude towards privacy.
* likely to use Facebook Apps as a means to explore, provided that they can learn doing so.
Conscientiousness
* cautious attitude towards disclosure of personal information.
* inot inlfuenced by group norms to a great extent.
* views social media as a distraction to attaining goals.
* less likely to use Facebook Apps, since they are generaly cautious about sharing personal information and may view it as a distraction.
Neuroticism
* more aware if the acquisition of knowledge if it favours themselves.
* can be influenced by others.
* more positive attitude towards privacy due to cautious disclosure.
* worrisome attitude likely to dissuade intensive use, especially if more aware of risk to privacy.
Agreeableness
* highly concerned with the norms of the social group.
* concerned about the disclosure of personal information. Thus a positive attitude towards privacy.
* likely to use Facebook Apps if others are also doing so.

Figure 4.1: Summary of the core behavioural influences of personality traits

4.4 The exploitation of individual differences

Chapter 3 provided some historical context regarding the surveillance of data where some technological advances, such as databases and spyware, were discussed. However, Facebook Apps were mostly absent from this discussion simply because it did not exist at the time. In fact, Apps as a whole is a recent development. As such, even though individuals are genetically predisposed from a personality perspective, their environments have only recently been influenced by these Apps. Even surveillance as a concept in and of itself is not new. The panopticon and institutional surveillance has been around for quite some time (Wood, 2007). What is new, is the combination of Apps and surveillance towards increasing the commodification of the harvested personal information. It stands to reason that these new environmental influences would also exert some influence on personality in general. It is argued that these additional influences are not only hidden, but mostly unquestioned simply because individuals think this has always been the case. For contemporary philosopher Slavoj Zizek, it is precisely this hidden (and unquestioned) influence that is at the heart of consumer ideology (Žižek, 1989, p.41). Unlike the factory workers during the time of Karl Marx, social media users are not always aware as to how their personal information, as well as the content they create, is used and to what extent. Consider a factory worker during the industrial era. He or she creates a pair of shoes using a certain amount of labour-power, which the capitalist sells for profit determined by the exchange value of that commodity. For the most part, they are aware of this and are likely also to know the selling price thereof. Thus to a large extent, these processes stand apart from the factory worker's personality. For example, the capitalist does not directly exploit core individual differences, such as the need to communicate. This is not in the capitalist's best interest.

This is not the case in modernity, where Facebook users are not aware of the exchange value attached to the content they create as a prosumer. Thus at its core, Facebook users are also unaware of the value attached to their personal information. However, this does not necessarily make them dissatisfied with Facebook. At least not to the extent that they avoid using it. In this regard, it is argued that unlike the capitalist, social media corporates (like Facebook) directly exploit core individual differences that are a part of every individual's personality. One such individual difference is the need to communicate. To further placate users, most of these platforms allow free access to all their communicative features, as well as the ability to access some third-party Apps using Facebook credentials; provided that an individual supplies them with their personal information.

Because platforms, such as Facebook, entice users by appealing to their basic need to communicate (and form social relations), the influence of personality becomes even more important. In turn, this affects each personality trait, which together exert a greater influence on the intent to use Facebook Apps. As such, together with society's obsession with data (argued in Chapter 3), Facebook has managed to create a captured audience. Note that the exploitation of users' need to communicate is only really used as a first step towards the use of social media, like Facebook. Once logged on, all the user content is indexed and surveilled and because users have already supplied the platform with their personal information, users assume no further harm can be done. Henry Giroux (2015, p.111) provides an apt explanation of this when he states that,

> *"...willful amnesia has taken hold of the larger culture, allowing privacy to be recklessly redefined through the material and ideological registers of a neoliberal order..."*

Thus, the free market economy furthers the exploitation of even more individual differences, including the need to further accumulate and consume - in this case, social media generated content. It is almost as if social media corporates facilitate the amplification of greedy behaviour. This form of greedy behaviour is also exhibited by the platforms themselves. Social media corporates wish to accumulate more capital, and social media users wish to consume and create more content (this includes personal information). This, in turn, fuels social media corporates' desire to accumulate capital. This not only creates a never-ending cycle where both parties supposedly benefit, but also perpetuates the notion that the surveillance of personal information (via the exploitation of individual differences) is not only acceptable, but actually desirable - the soft sell alluded to in Chapter 3.

Although individuals, like Snowden, have raised much awareness of such surveillance efforts, users are still inclined to use social media platforms. As such, awareness is but one behavioural aspect that needs to be studied. Since the exploitation of individual differences leads to the formation of strong motives and attitudes towards social media and Facebook Apps in particular; it thus makes sense to try and understand which personality traits exert the most influence on a user's intent to use Facebook Apps in combination with awareness and the other constructs prescribed by the TPB. In all, it thus stands to reason that personality has a direct and pronounced influence on the intention to behave in a particular manner - specifically within the context of this study.

4.5 Summary

This chapter has provided an overview of various personality theories with a particular focus on the trait-centric approach. Evidence was provided to motivate the use of the Big Five as a means of assessment. Further theoretical backing was provided by illustrating how personality traits influence user attitude as prescribed by the TPB. After illustrating how personality theory aligns with the TPB, further evidence was provided of the behavioural influence of personality. The chapter concluded by delineating how the larger problem (highlighted in Chapter 3) aligns with an individual's personality traits. The following chapter discusses the behavioural influence of attitude, information security awareness and social norms.

Chapter 5

THE THEORY OF PLANNED BEHAVIOUR AND AWARENESS

"There is nothing to writing. All you do is sit down at a typewriter and bleed."

— Ernest Hemingway

This chapter provides an outline of the relationship between attitude, social norms, awareness, and behaviour - a crucial component of the larger argument and research model. It provides an initial overview of the theoretical underpinnings of the aforementioned behavioural aspects followed by sections focused on specific forms of surveillance (one being government surveillance). The chapter concludes by discussing the surveillance of data within the context of Facebook Apps.

5.1 Theory of attitude

5.1.0.1 Attitude formation

Although the TPB provides researchers with a definition of attitude, it does not provide any specificity in terms of what the attitudes relate to. Is it tangible objects or intangible ideas or concepts such as surveillance? For some social psychologists attitude is simply, (Bohner & Wanke, 2002, p.5),

> *"...a summary evaluation of an object of thought."*

This definition is somewhat problematic in the context of this study as it is rather abstract. For example, what is defined as an object? How does the evaluation take place? Additionally, Jafarkarimi et al. (2016) suggest that attitudes and the other judgement of values and beliefs that lead to their formation, are not only related to the morals/ethics of the behaviour in question, but also biological factors. Earlier (circa 1899) psychology textbooks refer to this as the influence of the cortical set. As such, attitude comprises affective, cognitive, and connotative behavioural responses as part of a unified and multidimensional construct (Ham et al., 2015). Together, these behavioural responses attribute to attitude's combined behavioural influence - stronger than that of subjective norms (James et al., 2017).

However, not all responses need be accounted for. For example, this study is predominantly interested in evaluating cognitive responses in relation to attitude. For example, item 64 of the final questionnaire asks respondents about the use of Facebook Apps and provides a Likert scale containing various levels of danger and risk. These are considered to be cognitive in nature (Bohner & Wanke, 2002, p.5).

Similar to Cattell's views of attitude, Bohner & Wanke (2002) also argue that attitude is constructed as required, given the situation at hand and thus are learned or assimilated as argued later in this chapter (Perugini & Bagozzi, 2001). It is thus likely that the same respondent may provide different answers to specific questions, depending on their attitude (thus mood) at that moment, as influenced by the aforementioned situation. In turn, this requires a means to accurately evaluate attitude while compensating for attitudinal changes (mood); hence, the use of a social desirability scale (Marlowe-Crowne) in this study.

Social desirability scales, such as the Marlowe-Crowne variants, provide a means for researchers to account for changes in participant moods (Perinelli & Gremigni, 2016). As such, it becomes possible to identify individual responses that are overly positive (faking good) or overly negative (faking bad). Considered to be statistically effective at detecting such *faked* responses, the Marlowe-Crowne scales are a popular choice and generally outperform newer social desirability scales such as the Impression Management component of the Balanced Inventory of Desirable Responding (BIDR) scale (Lambert et al., 2016). For these reasons this study makes use of a Marlowe-Crowne variant - specifically the scale developed by Ray (1984). To operationalise these scales a researcher decides on a threshold value beforehand. If the total score (of Likert-based items) are either very low or very high the respondent's responses are deemed socially undesirable and may be discarded.

There is also evidence that the formation of attitudes have a genetic component. This, however, requires the behavioural response to be culturally agnostic and not be experiential in nature. Given the widespread use of Facebook and its culturally agnostic appeal (van der Schyff et al., 2018), it is plausible that attitudes towards Facebook is influenced by genetics. Interestingly, this coincides with the genetic influence of personality as studied by Eysenck. However, evidence to substantiate such a claim is based mainly on the work of evolutionary psychologists. For example, in general, humans prefer abundant vegetation and forests as opposed to dry and barren landscapes. Physical attraction also supports the genetic influence of attitude across different cultures. Furthering this genetic argument, research has found that both men and women calculate behavioural costs beforehand. For example, behavioural cost (psychological and physical) of having children is higher for women than men. Hence, the formation of different attitudes towards having children (Bohner & Wanke, 2002, pp.73-75). This makes the inclusion of gender and attitude interesting within the context of this thesis, since theory suggests that women are more cautious overall. One would expect this to apply to Facebook Apps as well. No environmental or situational cues are presented to respondents (in the questionnaires), which may favour the genetic influence of attitude in this context.

Moreover, several attitudinal relationships have been shown to correlate with genetics, such as interest, authoritarianism, and patriotism (among others). If one considers excessive interest as a form of dependency, then it stands to reason that Facebook use, and even consumerism are also genetically influenced to some extent. In Chapter 4, the genetic influence of personality was briefly discussed by referring to the work of Eysenck. A trait-centric personality approach (thus dispositional) was motivated, forming the core of the resultant discussion on the behavioural influence of personality on attitude. In this regard Bohner & Wanke (2002, p.75) provides an apt summary stating that,

> *"People form attitudes that are compatible with their dispositions, such as personalities and abilities."*

5.1.0.2 Attitude change

Once formed, how does a change in attitude take place? One such method would be to align any persuasive efforts to the functions served by the attitude in question (i.e., as per the functional matching hypothesis). However, the same or similar attitudes could serve different purposes. For example, a Facebook user may oppose social media surveillance because of social norms (they wish to fit in), or it limits their ability to conduct phishing campaigns (utilitarian) or simply because they are in favour of their right to privacy (a value judgement).

In all three instances, the Facebook user has or forms a negative attitude towards Facebook surveillance. Thus, bringing about effective (and lasting) change requires a specific and targeted approach. Kelman (1958) views persuasion as a latticework of social influence - specifically the concepts of compliance, identification, and internalisation.

5.1.0.3 Change due to compliance

For Kelman (1958) lasting attitudinal change takes place at different levels, each associated with a different process of individual acceptance. As such, it is possible to perceive the same overt behaviour, although it is the result of various combinations of behavioural processes (induced behaviour). Induced behaviour takes place to produce or lead to the perceived overt behaviour.

By this definition one could assert the following within the context of Facebook Apps: A user makes use of a third-party App developed by his or her insurance company so that they may be rewarded for good driving behaviour. Recall that by definition, such a third-party App is also regarded as a Facebook App, provided that the user is permitted to sign in with their Facebook credentials. In this example, the user strives to behave in a manner dictated to him or her by the insurance company (induced behaviour). If deemed compliant the individual is rewarded accordingly. From the individual's perspective, the content (telemetry data) is unimportant as long as the reward is obtained.

Although Kelman (1958) refers to sanctions if the behavioural responses are not favourable (i.e., they do not lead to the desired overt behaviour) sanctions do not fit within the theoretical confines of the TPB - a limitation in this context. Similar examples of Facebook-authored Apps could also be used. For example, some users may play Facebook games for the thrill -

it may even become a form of dependency. The actual game (thus content) is not of importance as long as the user enjoys the game psychologically (the thrill). The same user may also feel that they have to comply with others within their circle of influence. The App is thus used because of social norms. Importantly, no matter what the attitude was before using the App, the behavioural responses required to comply (induced behaviour) results in the actual use of the App (overt behaviour). As such, attitude change has taken place due to the *compliance* aspect of social influence.

5.1.0.4 Change due to identification

As a second form of social influence, Kelman (1958) discusses the concept of *identification*. Whereas compliance seeks to reach favourable behavioural responses, identification aims to build a relationship in the process. Individuals believe in their behavioural responses as part of the relationship's identity. As such, individual behaviour is adapted to align with these relationships. Here, there are elements of both descriptive norms and awareness. Users may use Facebook Apps, such as Facebook Messenger, not only because they wish to comply, but also because they wish to identify with those already using the App (descriptive norms). The actual behavioural responses (induced and overt) are not of concern, but rather a means to identify with the group. In turn, a positive change in the user's attitude towards the use of Facebook Messenger has taken place.

5.1.0.5 Change due to internalisation

Attitude change can also take place through the process of *internalisation*. This occurs when the content (ideas and values) are viewed as something of value to the individual. As such, the resultant behaviour is aligned with the individual's beliefs. Using aspects of the previous examples, individuals may initially play Candy Crush Saga, but cease using it when becoming aware of the personal information being misused. Such a user may hold privacy rights in high regard, leading to a negative attitude towards Facebook App surveillance once the new information has been internalised.

5.1.1 Theoretical integration of attitude

This section outlines how both attitude and personality theory integrates with the Theory of Planned Behaviour (TPB); specifically how Cattell's ergs and sentiments influence attitude formation and change - a process referred to as subsidiation (Schultz & Schultz, 2004, p.281).

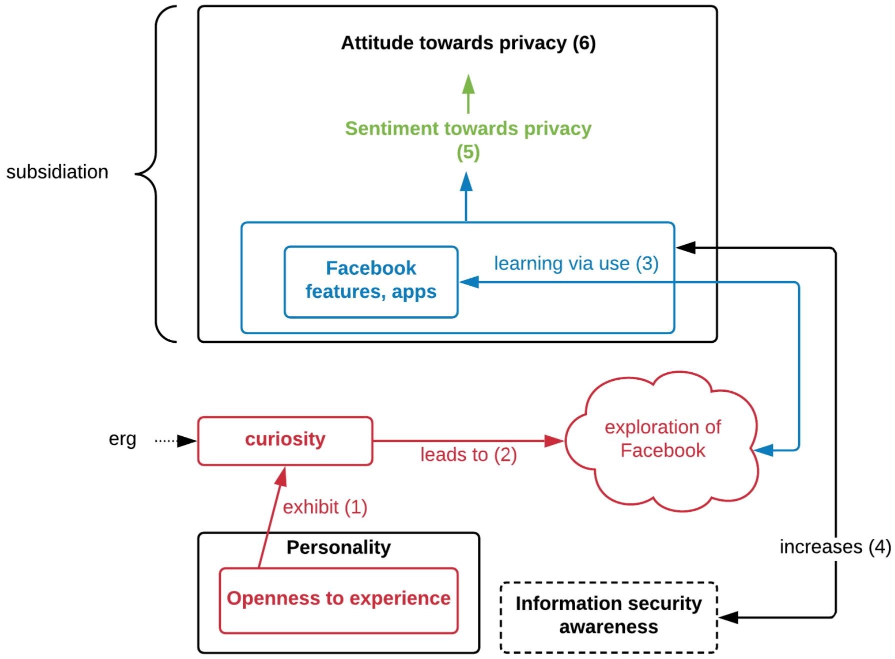


Figure 5.1: Process of subsidiation

In Figure 5.1, the process of subsidiation is illustrated by making use of Cattell's ergs, sentiments, and Openness to Experience as a personality trait. It is argued that, because both Cattell (as well as Costa and McCrae) used factor analysis of lexically derived factors, this explanation also applies to other trait-centric approaches (i.e., such as the Big Five). Note that Figure 5.1 only illustrates how personality theory integrates with attitude and the TPB. It does not attempt to explain how specific factors and ergs are related to each other.

5.1.1.1 Assessment and alignment issues

To illustrate why the mapping between factors and ergs may be problematic, consider the possibility that anger (an erg) can be mapped to more than one trait within the Big Five. For example, anger could be associated with Neuroticism - the result of prolonged stress and anxiety, which are both hallmarks of Neuroticism. Using ergs in this manner limits being able to label or classify an individual using one lexical term. Do we label this person as one high in Extraversion or high in Neuroticism? To some extent, this can be addressed by examining the means of assessment. Much of Cattell's work is based on survey data. For surveys to be able to distinguish between the two factors, it has to consist of enough items (questions) to be able to eliminate certain traits. Hence the need for instruments that are expansive enough to eliminate irrelevant traits. This, in turn, has led to the creation of several assessment instruments. For example, the commercial versions of the Big Five instrument is referred to as the NEO PI-R. The NEO PI-R instrument consists of 240 items and is not strictly used for research, due to its length. For this reason, several other alternatives exist with varying lengths ranging from 10 to 100 items.

As such, the emotive classifications (such as anger) is not useful as the primary means of understanding (thus assessing) an individual's attitude towards privacy. Assume that the current study proposes the use of an instrument incorporating only specific individual differences, such as anger. However, upon concluding the study, no conclusive inferences could be made from the survey data. One explanation could be that the survey respondents were mostly high in Conscientiousness, Openness to Experience, or Agreeableness. These traits are, however, not significantly correlated with individual differences based on anger. This means that the study would have evaluated an irrelevant individual difference. Another unrelated example is the use of the Dark Triad to explain the intention to engage in community engagement efforts. The Dark Triad is inherently negative, which does not align with an altruistic, positive, and selfless activity such as community engagement.

5.1.1.2 Subsidiation in context

Subsidiation is a process that defines the formation of attitude as an interplay between ergs and sentiments. Sentiments are learned and directed towards an object or abstract concept. Importantly, sentiments are not permanent personality structures and may disappear altogether over time. Conversely, ergs are innate (and permanent) psychological dispositions that cause an individual to react and experience emotion at different levels, depending on the class of object it is in relation to. For example, one individual may like social media and thus possess a heightened sense of curiosity about social media. From the previous chapter it follows that an individual high in Openness to Experience is naturally curious (curiosity is an erg) and likely to explore new technologies (step 1 and 2 in Figure 5.1). When the individual decides to start using Facebook (step 3), their curiosity will lead them to learn about specific Facebook features and Apps by using the platform. In turn, it likely that this learning process will also increase the level of information security awareness when using Facebook Apps (step 4). This is illustrated as a bi-directional relationship, since an increase in awareness is likely to highlight additional areas of interest. In turn, this additional awareness leads to more learning and exploration - and so the cycle continues. Importantly, when the this individual reaches step 4, he or she has formed a sentiment towards Facebook Apps and information privacy (step 5). This sentiment then leads to the formation (or change) of an attitude towards privacy (step 6). Over time, this attitude could change (positively or negatively) or may disappear altogether depending on user perceptions.

5.1.1.3 Limitations

Thus far, the discussion has focused on specific personality dimensions (Conscientiousness and Openness to Experience) and integrated it with the work of Cattell. This was then transposed onto the TPB to illustrate its relevance within this context. At this stage specific questions may come to mind. For example, why use the theoretical work of Cattell? Furthermore, why not use Cattell's 16PF personality instrument?

Firstly, most of the ergs are based on an emotion or verb. If an individual is classified as angry, curious, and gender, how is gender going to assist in explaining the influence of personality? It would have to be mapped to a personality trait, but which one? As alluded to earlier, it is difficult to focus on a specific erg or individual difference before first exploring the general behavioural influence of broader traits (such as the Big Five). The same applies to the erg named hunger. Additionally, some of the 16PF factors are not well suited for this study. An individual's level of submissiveness or dominance would not likely directly influence awareness; primarily if the process of becoming aware is not enforced or monitored as is the case with corporate information security policies. Within this context, an individual's level of awareness is mostly influenced by others in their circle of influence (social norms) and how much they know or learn about it (sentiments as part of attitude). This, in turn, is a function of how much the individual in question wishes to know. If they are apathetic in this regard, their learning will most likely not take place. In addition to these, motivation is also not directly integrated into the TPB, although it appears in personality theory. The same applies to habits, which form the constituent components of an individual's personality, according to Allport (Schultz & Schultz, 2016). These habits are then classified as either part of the perseverative or propriate functional autonomy. The perseverative functional autonomy is mainly driven by habits but does not form an integral part of personality. Conversely, those habits deemed part of the propriate functional autonomy are central to personality-driven behaviour. Although a detailed explanation of these concepts are provided, they do not directly inform attitude formation or change towards a behaviour or object (Allport, 1931). This further limits integrating Allport's personality theory with the TPB.

5.2 Behavioural influence of attitude

Thus far, the discussions have centred on attitude theory and contextualised it within the TPB. In line with this study's research model, the following section discusses the behavioural influence of and relationships to and from the construct named *Attitude towards privacy*. Furthermore, Figure 5.2 provides a visual map as to how the literature in this chapter aligns with the items in the research instrument. It specifically illustrates:

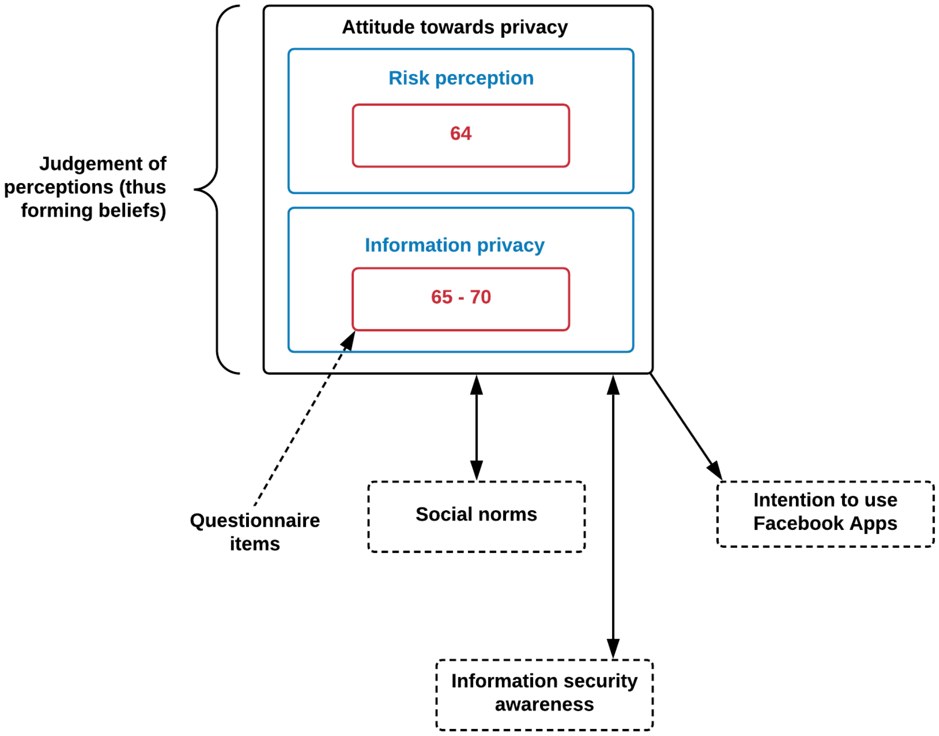

Attitude towards privacy
Risk perception
64
Information privacy
65 - 70
Judgement of perceptions (thus forming beliefs)
Questionnaire items
Social norms
Intention to use Facebook Apps
Information security awareness

Figure 5.2: Alignment of *Attitude towards privacy* with the questionnaire items

- How the attitude-centric items are grouped (blue rectangles in Figure 5.2), and
- The main cognitive function (perception) that produces the stimuli to be judged within the context of the research model construct - *Attitude towards privacy*. Note that within the context of this study, perception is defined as [1],

  > *"The way in which something is regarded, understood, or interpreted."*

- Lastly, Figure 5.2 also illustrates how *Attitude towards privacy* is integrated with the TPB.

Although the following subsections are aligned with Figure 5.2, they are blended with studies that also discuss information security and general awareness studies. Literature on the influence of social norms is also included. This further aligns the entire section with the research model of this thesis.

5.2.1 Risk perception

Although the TPB does not directly address the perception of risk, it plays an important role. To illustrate this, consider employees' intention to comply with information security policies. Here, employees have to perceive several factors that may influence their attitude towards compliance. In this regard, employees have to perceive concepts such as consequences of non-compliance, possible sanctions, and vulnerability. According to some authors, these factors (among others) are influenced by awareness, which in turn directly influences attitude (Park et al., 2017; Tsohou et al., 2015). For example, Tsai et al. (2016) posits that individuals who are more aware of threats (and the risk they pose) are likely to perceive themselves as adequately equipped to mitigate these threats. It is thus plausible that these individuals are less likely to adopt security software or behaviour, since they are more confident in their coping abilities. In contrast, Conger et al. (2013) suggests that individuals attitude towards personal information may change as they perceive risks (increased awareness), such as the misuse of their personal information. Saridakis et al. (2016) agrees adding that a heightened perception of risk (on social media) cultivates a positive attitude towards secure behaviour.

[1] https://en.oxforddictionaries.com/definition/perception

Similar findings are portrayed by Ki-Aries & Faily (2017) who found that individuals lacked the requisite knowledge to make informed security decisions. Additionally, those individuals who did adopt secure behaviours believed they were not adequately rewarded. As a result, these individuals were less inclined to engage with internal security guidance. Although this is not strictly due to risk perception, the resultant insecure behaviour of these users illustrates both ignorance and wilful amnesia post perception.

As such, where these users once perceived risk in behaving insecurely, they now deliberately behave otherwise - an adverse change in their attitude towards secure behaviour. For Williams et al. (2017) such forms of risk perception hinge on the notion of beliefs, which encapsulate the former. Although Williams et al. (2017) refers to beliefs their argument soon equates this to the cognitive function of perception. Following this, perceived anonymity is used as an example to illustrate the effect thereof on self-disclosure (information sharing) within online environments.

5.2.2 Privacy of personal information

Notwithstanding the moral connotations (i.e., whether it is good, unnecessary or required as per questionnaire items) Facebook users hold that regard to the platform's access to their information, information privacy is generally a contentious subject (Fuchs, 2011). People, fuelled by Western beliefs believe that privacy is to be considered a human right that is to be desired (Bergström, 2015). Together, such ideological notions directly influence the concerns individuals harbour concerning the privacy of their personal information. Importantly, these concerns exist in theory; they do not always guide resultant security behaviour - a privacy contradiction referred to as the privacy paradox.

The privacy paradox states that users' intentions and actual behaviour are sometimes mismatched when it comes to securing their personal information (Kokolakis, 2017). On the one hand, it is deemed as vitally important, yet it is readily proffered - especially when something is to be gained when relinquishing access to one's information. This again ties into the usefulness of social desirability scales. Nonetheless, it is common for e-commerce merchants and social media platforms alike, to appeal to individuals' propensity to trust others when experience has proven people's tendency to be honest. This is commonly referred to as truth bias (Bergström, 2015; Williams et al., 2017). Self-regulatory and transparent mechanisms are employed by the parties mentioned above to instil a sense of trust, by proving explanations about the secondary use of personal information (Vladlena et al., 2015). This includes the use of privacy policies, even though users may perceive them differently (i.e., they do not allow direct control of information).

Such mechanisms not only ameliorate privacy concerns, but also increase the likelihood that additional expenditure may take place on these websites. Authors, such as Bartsch & Dienlin (2016), propose increasing individuals' privacy literacy as yet another mechanism to increase privacy awareness. These mechanisms could also have the opposite effect. For example, users' concerns over the use of their personal information may increase, since they are now fully aware of the extent that it is used (Karwatzki et al., 2017). Moreover, the easier it is to locate privacy information, the more sensitive the matter becomes (Wagner et al., 2018). Together, the heightened awareness and increased sensitivity leads to a reassessment of the risks and benefits associated with continued use of the website in question. In turn, the resultant learning that takes place either influences their attitude negatively or positively. Here, James et al. (2017) found that among both American and Chinese participants, their concerns over the privacy of their information and level of awareness positively influenced participants' attitude towards instant messaging.

These levels of positivity and negativity are determined by the relationship between the construct named *Attitude towards privacy* and that of *Awareness of information security*, as dictated by this study's research model. From the researcher's perspective, this is a positive consequence - one which addresses both the *wilful amnesia* alluded to in Chapter 3 and the ignorance users display towards the security of their personal information.

Some authors also make the distinction between awareness of policies, guidelines, best practice, and legal requirements. It is not a legal requirement for social media users to be concerned or even knowledgeable about the privacy of their personal information (Park et al., 2017). This also contributes to the amnesia mentioned above, since ignorance in this regard is not an offense. Together with the belief that their personal information is of no value, users develop a *don't care* attitude towards information privacy. As such, social media surveillance is not seen as a malevolent practice, but rather something benevolent - a means to combat fraud and terrorism. In contrast, awareness of specific threats (as part of an appraisal process) has been shown to positively influence users' attitude towards passwords (Mamonov & Benbunan-Fich, 2018). However, the research above is not explicit about the nature of these threats. If interpreted as legal, this may account for such contrasting findings. Notwithstanding these specific aspects of threat appraisal and awareness, it is largely users' propensity to speculate and base decisions upon assumptions that typifies their attitude towards information privacy. Information devoid of specifics, such as intended use and decision consequences also influence individuals' attitude towards the privacy of their personal information (Hirschprung et al., 2016).

5.2.3 Institutional trust

Although the concept of trust is multidimensional and no two individuals have the same understanding thereof, it forms a core (latent) component of not only this study, but social media in general (Pentina et al., 2013). It stands to reason that the polarity of an individual's attitude, influences their level of trust. This view of trust sets it apart from the debates as to whether or not it should be viewed as an antecedent or consequence of information privacy concerns (Kehr et al., 2015). Within the context of this study, the TPB provides us with a means to argue that trust could be regulated by the bidirectional relationship between attitude and awareness - thus acting as both an antecedent and consequence of information privacy concerns. It acts as a consequence when websites and social media platforms implement mechanisms (transparency, for example) to cultivate a positive attitude towards the privacy of their personal information. On the other hand, it acts as an antecedent when influenced by other individuals within the user's circle of influence - as per the TPB's relationship between attitude and subjective norms (Kokolakis, 2017).

According to Kehr et al. (2015), the aforementioned is specifically referred to as institutional trust and is primarily determined by the level of confidence users have that these websites or social media platforms will not misuse their personal information. Here, confidence refers to the tendency to trust the organisation (such as Facebook) collecting the information, subject to the outcome of the aforementioned risk-benefit analysis. For example, Zimmer et al. (2010), found that risk perceptions declined when websites requested personal information users believed to be relevant. Staiano et al. (2014), found that users could rank organisations based on the level of institutional trust. Some research even suggests that the trait of information being disclosed is more important than the organisation disclosing it. As such, users are more likely to supply personal information (even sensitive) to organisations that are deemed trustworthy (Junger et al., 2017). This, in turn, results in a positive attitude towards disclosing personal information.

Experience with privacy invasion also influence users' attitude towards the disclosure of personal information (Taneja et al., 2015). It is likely that negative experiences not only lead to a change in attitude, but also influences users' stance towards responsibility. For example, Miltgen & Peyrat-Guillard (2014) found that the aspects above differ, based on an individual's country of residence. Internet use (a form of experience in their study) in France was found to be positively related to responsibility, but not trust. Conversely, users in Greece use the Internet less. Therefore, it stands to reason that these users lack the experience of those in France; hence the emphasis on trust (i.e., they feel compelled to trust because they do not know any better). Here, awareness (thus knowledge and understanding) is lower, which in turn influences attitude and resultant information disclosure.

Importantly, Miltgen & Peyrat-Guillard (2014) argues that trust should be viewed as an antecedent, but also places emphasis on responsible information disclosing behaviour - something shared by users and corporates alike. Even though Miltgen & Peyrat-Guillard (2014) proposes that trust should be viewed as an antecedent, there is an element of coercion. Here, Polish and Estonian participants stated that they had no choice but to trust certain organisations (such as banks, government, and major corporations). Miltgen & Peyrat-Guillard (2014) refers to this as *forced consent*, similar to this study's *ontological dilemma*. In this manner, Baudrillard's *real* (Baudrillard, 2016) (consumerist in nature), is transposed onto the user's reality, which may or may not align with the former. Of course, this depends on the individual in question; hence, this study's investigation into how these individual differences influence user perception.

Consumer reality requires (even demands) personal information. Some users provide this information without question, while others do so reluctantly. It is precisely the latter group of users who directly face the dilemma mentioned above. Their reality (primarily determined by their beliefs and attitude) does not align with that of the consumer society at large. Such ideologically driven influences on user attitude also extends to the relationship between political orientation and information disclosure. For example, Bergström (2015) found those leaning to the political lefthad more concerns regarding the possible misuse of their personal information (on social media) than those right oriented.

Overall, trust plays an important role, explicitly when perceiving the amount of risk inherent in the exchange of personal information. As these levels of trust increase, so does the behavioural intent to disclose personal information (Bansal et al., 2010; Posey et al., 2010).

5.3 Theory of social norms

Social norms, as defined by Lapinski & Rimal (2005), includes both descriptive and injunctive norms that influence the formation of beliefs that emerge from the interactions between members of a social organisation. Social norms not only function as a means to encourage involvement within the social organisation, but also cultivate responsibility in terms of individual actions (Minton et al., 2018). For example, social norms act as guiding principles which these members have to follow. As such, the members of s social organisation take it upon themselves to regulate their own behaviour in line with the extant social norms of the organisation. From a contextual perspective, if specific components of an individual's personal information is visible to all of his or her Facebook friends, the onus is on the individual to secure the information. There are, however, instances where the use of Facebook Apps impact other users - specifically those within an individual's friends list (Symeonidis et al., 2018). These Apps harvest personal information from friends and vice versa. Using this example, the interplay between the responsible use of specific Facebook Apps within a familial environment and the social norms within this social unit is likely to influence the use of these and similar Facebook Apps. However, these individuals may not be aware that certain Facebook Apps perform surveillance of personal information in this manner. This makes the inclusion of awareness of particular importance in this study.

From a theoretical perspective, injunctive norms are inherently prescriptive. In turn, this makes it possible to include subjective norms. As such, both descriptive and subjective norms form part of social norms - both theoretically (Ham et al., 2015; Lapinski & Rimal, 2005) and in this study's research model (see Chapter 6). Descriptive norms is defined as behaviour that is currently taking place (Ham et al., 2015), whereas subjective norms are defined as an individual's belief as to how others think they should behave (Thompson et al., 2017). For example, if an individual observes his friends, family, or other people using a specific Facebook App, it is plausible that the individual will also make use of the Facebook App (descriptive norm). On the other hand, if the same individual is a fitness enthusiast, the individual might use Facebook Apps to track his or her fitness levels, simply because fitness enthusiasts are expected to use such Apps (subjective norm). In this study, social norms are evaluated by questions 71 to 77 and explores the influence of friends, family, or people in general (see Figure 5.3 for more detail).

To further motivate the evaluation of the combined influence of subjective and descriptive norms, consider the use of Facebook Apps based on the following: Some Apps are presented in the Facebook App Center (web and mobile version). For the most part, these Apps indicate how many other users are using the App. This is especially pertinent for the Facebook Apps that are gamified. Importantly, these Apps allow users to comment, review, share, and view feeds of other users playing or using similar Facebook Apps. These mechanisms (forms of enticement) favour an experiential approach. For example, users cannot fully appreciate the influence of these mechanisms without actually using the Facebook App Center. It is however, precisely this experiential nature of Facebook Apps that make it difficult to ascertain whether the users, who are commenting, are actually using the App (descriptive) or just commenting (subjective). Hence, although there are subtle theoretical differences (outlined below), this study assumes that Facebook users are unlikely to make these distinctions before enacting their intention to either use or avoid Facebook Apps. As such, this study is not concerned as to how Facebook users perceive these differences, but rather the resultant influence on intended behaviour as a whole.

5.3.1 Theoretical integration of social norms

This section outlines how social norms integrate with the TPB. It also discusses how other studies have made use thereof, by explicitly focusing on theoretical integration within other contexts. As stated above this study views social norms as a construct comprising both descriptive and subjective norms. They are however, not evaluated separately because of the subtle behavioural differences - both theoretically and contextually, in this study.

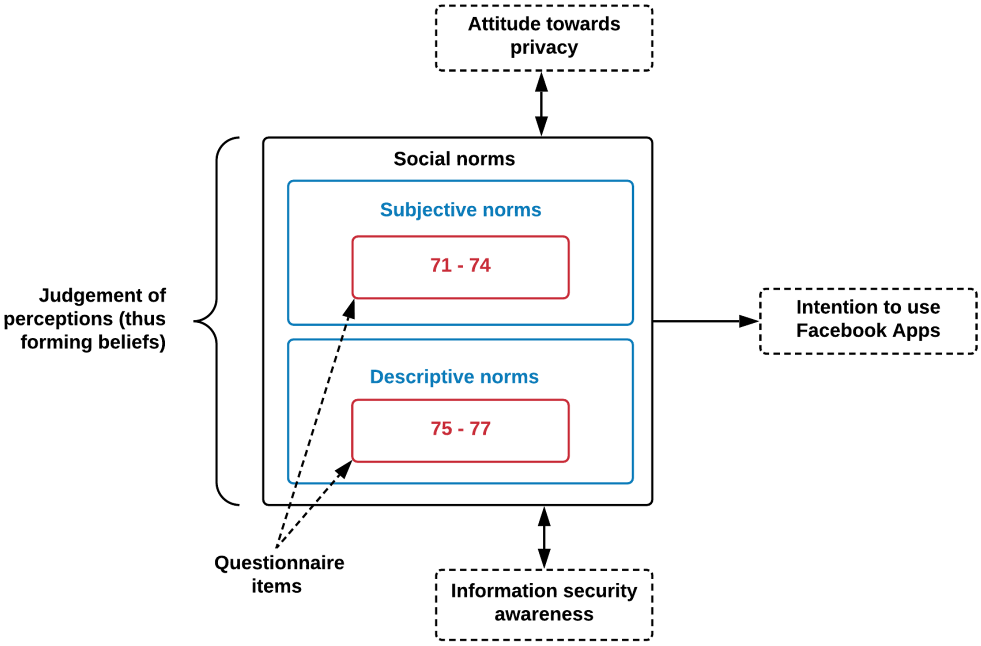

Attitude towards privacy
Social norms
Subjective norms
71 - 74
Descriptive norms
75 - 77
Judgement of perceptions (thus forming beliefs)
Intention to use Facebook Apps
Questionnaire items
Information security awareness

Figure 5.3: Alignment of *Social norms* with the questionnaire items

5.3.2 Subjective norms

Although proven to be a weaker influence on behavioural intent than attitude, subjective norms refer to beliefs related to others' approval of a behaviour (Chandran & Aleidi, 2018) or the perceived social pressure to behave in a certain way (Taneja et al., 2015). For example, a Facebook user may avoid Facebook Apps related to gaming, simply because the users believe their families will disapprove thereof. Morris & Liu (2015) refers to this as a type of herd mentality, where individuals are easily influenced by the larger social group - specifically behavioural patterns exhibited by the majority and elite within the social group. Enacting these behavioural patterns not only strengthens group identity, but also achieves large-scale consensus and validation; especially when individuals adhere to the norms of the majority (Morris & Liu, 2015). Endorsing norms favourable to the use of Facebook Apps within the majority of a social group is thus likely to exert a more significant influence on the intention to use these Apps, within the social group in question.

Fundamentally individuals' desire to enact subjective norms within a group is a function of insecurity. As such, any motive to adhere to group norms is influenced by one or a combination of the following forms of insecurity: social identity, epistemic, or existential (Morris & Liu, 2015). There are other influencing factors; one such example being egoism. For example, Minton et al. (2018) found that specific individuals would adopt behaviours indicative of sustainable consumption because it enhances their self-image, rather than actually being concerned for the environment. Such behaviour also ties in with attitude change or formation within the context of the TPB. Individuals may decide to adopt behaviours indicative of sustainable consumption, not because they believe it is prescribed by the rest of the sustainable consumption community, but rather to improve their own self-image (i.e., to be seen as an environmentalist) (Minton et al., 2018). These individuals only abide by the community's subjective norms because it serves a covert purpose. Either way, subjective norms have influenced their behaviour, which in turn also influences their attitude towards these behaviours - as illustrated by the bi-directional relationship between attitude and subjective norms in the TPB.

Although adherence to subjective group norms can be beneficial, it does engender some drawbacks. As an example, consider the concept of creativity. If everyone in the group behaved similarly, it is likely that the group would display very little (if any) creativity. Some individuals may also feel that it distances them from that which makes them unique. Individuals high in Openness to Experience may feel that excessive adherence to prescriptive group norms limits their natural sense of creativity. Consider the use of Pinterest (a third-party Facebook App) within a familial environment. If the family considers the use of third-party Apps to be unsafe, those family members high in Openness to Experience may feel unhappy in that it limits their curious nature. This does not, however, guarantee that such individuals will always comply with group norms in this manner. In fact, some group members may decide to behave in a manner that counters each and every accepted group norm (Morris & Liu, 2015).

Within the context of Facebook Apps, it is thus plausible that an individual high in Neuroticism may use gaming Facebook Apps to exude a playful demeanour - something they are unlikely to display offline. As such, these individuals play these games not only because they believe it to be desired by others, but also to make others think they are fun and playful (i.e., for covert purposes).

5.3.2.1 Behavioural influence of subjective norms

As per the previous discussion, many subjective and descriptive norms centre on the beliefs of individuals; either on what they believe others think or believe as to what they do. These beliefs not only allow researchers to differentiate between subjective and descriptive norms, but also influence behaviour. This is especially important within the realm of social media, where subjective norms significantly influence intended use (Lee et al., 2016). Either directly as an influence on behavioural intent or indirectly, by influencing perceived behavioural control and attitude. For example, Kusyanti et al. (2017) found that the more other users believe in Facebook, the more likely new or existing users are to use and trust how these platforms manage the security of their personal information.

As is the case with attitudes that are faked, individuals may also exhibit behaviour that they believe to be desirable within that social setting. Their beliefs pertaining to what others deem acceptable, thus guide their resultant behaviour. Even if it does not reflect the truth. A case in point being an Australian study which found that users generally provided positive responses (i.e., faking good) to questions regarding security incident response regardless of the actual circumstances surrounding those incidents (Parsons et al., 2017). To quantify the resultant effect of these overly positive responses Parsons et al. (2017) used the same 8-item Marlowe-Crowne variant as this study. It was explicitly decided to investigate those behavioural aspects of their model further if the correlation co-efficient were over 0.25. Similar to the covert purposes alluded to earlier, Parsons et al. (2017) concluded that respondents' overly positive responses are based on an Australian norm, which states that it is not socially acceptable to report on the behaviour of others, regardless of polarity (i.e., good or bad).

Similar culture-based studies have also indicated that collectivist social groups are more likely to behave in a manner representative of those subjective norms accepted by the social group in question. This is even more pronounced when individuals share attributes with the rest of the social group (Pentina et al., 2013). In turn, this aligns with Kelman's view of attitude change via the process of *identification*.

Identity formation within familial environments also significantly influence resultant behaviour. For example, Kisyovska et al. (2015) found that individuals within dysfunctional families exhibit greater tendencies to become dependent on Facebook. Here, individuals wish to enact covert behaviour so as to escape the aforementioned negative familial, social pressures. James et al. (2017) also acknowledge the role of social enhancement. They argue that social media users may develop obsessive behaviours, not because of familial pressures, but rather because their perceptions of how inadequate they are based on comparisons with information shared by other members. Such feelings of subjective inadequacy further stimulate the obsessive use, since these users feel the need to engage, so as to overcome these feelings continually. This leads to the formation of positive attitudes towards information disclosure - albeit for competitive or covert reasons. These findings further motivates the influence of subjective norms on attitude (as per the TPB) (Mamonov & Benbunan-Fich, 2018). Staiano et al. (2014) provides further evidence in this regard by also tying in with Kelman's work on attitude change - precisely the concept of *internalisation*. For example, the disclosure of different traits of personal information by others has been shown to influence an individual's attitude. This stands in contrast to individualistic cultures, that are less likely to be influenced by group norms (Posey et al., 2010), as well as on the need to identify with others.

Recommendations as a form of subjective pressure have also been found to influence how social media users disclose personal information - specifically location-based information. For Chang & Chen (2014) the decision to disclose location-based information is influenced by both attitude and subjective norms held within the social group. If a social group exhibits a positive attitude towards location-based disclosure (by recommending it), then it is more likely that group members will share this positive attitude. In turn, these users are more likely to participate in location-based disclosure. Another example which illustrates the role of recommendations can be found when one considers electronic word of mouth (posts on social media). For example, Shan & King (2015) found the subjective influence of family and friends to be stronger if they recommend a product, as opposed to other forms of influence (i.e., advertisements). This again relates to the concept of trust. Even though an individual may not have any experience with the product, they are more likely to use/buy it because they trust the judgement of their family.

Although this represents an indirect form of trust, it still influences an individual's behavioural intent. Similarly, social media users do not intend to continue using a specific platform like Facebook because they trust the platform, but rather because they have become accustomed to and trust the members that form part of the social relations they have formed while using the platform (Chen et al., 2016).

Over and above familial influence, age also influences to what extent individuals adopt subjective norms within a social group. For example, Chakraborty et al. (2013) found that older adults are more likely to share personal information on social media if other older members are perceived to share their personal information.

5.3.3 Descriptive norms

Based on the perceptions of what others are doing, descriptive norms form an essential part of this study. Acquired using a combination of both experiential and conceptual influence, descriptive norms also takes into account the context of the behaviour being enacted (Benson et al., 2015). The more information is perceived about enacting a behaviour; the more likely other individuals are also to enact that behaviour (Junger et al., 2017). Evaluating the behavioural influence of descriptive norms has proven especially useful for some researchers. In a social proof-based study Das et al. (2014) demonstrated to Facebook users how their friends were making use of security features (i.e., privacy settings for example) and found it to be more effective than making them aware of specific security issues. The same behaviour was observed offline. For example, when Junger et al. (2017) asked individuals to disclose their personal information via a physical questionnaire in a public environment, they did so readily when enacting the behaviour in groups or after observing the majority of the group disclosing their personal information.

5.3.3.1 Behavioural influence of descriptive norms

Unlike Ham et al. (2015); Rhodes & Courneya (2003), this study does not include descriptive norms as part of subjective norms, but rather evaluates it separately as part of the construct *Social norms*. Separation in this manner is supported in literature (Taneja et al., 2015), which indicates that descriptive norms are a significant predictor of behavioural intent. More so than subjective norms in some contexts. For example, Thompson et al. (2017) found security intentions among home and mobile users (of personal devices) to be significantly influenced by descriptive norms. Lee et al. (2016) refers to this as social presence confirming that the perception of others (peers and family) using social media significantly influences the intention to use said platforms. Conversely, subjective norms have been proven to be a better predictor in work environments due to its prescriptive nature (i.e., as dictated by superiors) (Godlove, 2012). Because Facebook Apps could be used in both a personal and professional capacity, it is likely that both subjective and descriptive norms will exhibit a behavioural influence rather than subjective norms.

Although the aforementioned security studies indicate the importance of descriptive norms over subjective norms, there is at least some evidence that they are equally important in predicting behaviour. For example, Ham et al. (2015) indicates that an individual's intention to purchase *green food* is significantly influenced by both social and descriptive norms. Unlike the theoretical stance of Lapinski & Rimal (2005), Ham et al. (2015) argues that social norms form part of subjective norms, alongside descriptive norms. Theoretically, this implies that social norms, as a whole take on an injunctive role. Because injunctive norms and subjective norms are inherently prescriptive, describing those norms that are already prescriptive does not make sense in this context, simply because describing behaviour which is prescribed merely acts as a description of the behaviour and not a predictor thereof.

5.3.4 Social norms in retrospect

Because of the subtle difference between subjective and descriptive norms, it is likely that the five personality traits perceive them similarly. For example, users high in Agreeableness and Neuroticism are likely to enact behaviour that is both described and prescribed (subjective) from a personality theory perspective. Furthermore, because it would require academic effort to recognise and understand the difference between the two norms entirely it is likely that only individuals high in Conscientiousness will answer these questions differently; hence, the evaluation of how the five personality traits influence social norms consisting of both descriptive and subjective norms.

5.4 Theory of information security awareness

Within the context of this study, information security awareness is evaluated by items 78 to 89 (see Appendix A), in the form of three scales adapted from several other studies. Although these scales differ in their wording and overall approach, they all evaluate an individual's awareness of the security of their personal information stored or used by their Facebook friends and Facebook (the platform). Additionally, since these items capture thoughts based on perceptions, the same cognitive processes apply as with the other items and constructs (see Figure 5.4).

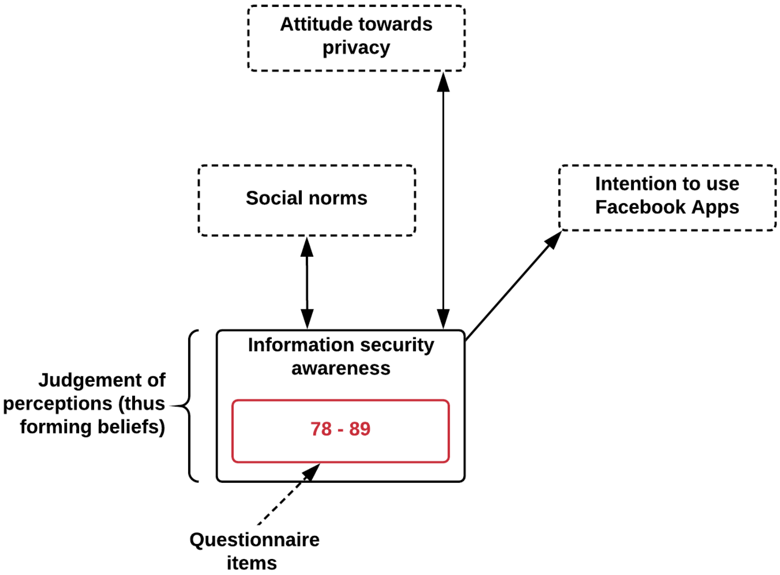

Attitude towards privacy
Social norms
Intention to use Facebook Apps
Information security awareness
78 - 89
Judgement of perceptions (thus forming beliefs)
Questionnaire items

Figure 5.4: Alignment of *Information security awareness* with the questionnaire items

5.4.1 Theoretical integration of awareness

In this study, *Information security awareness* is evaluated instead of Perceived Behavioural Control (PBC) - a theoretical contribution in this context. Within the TPB, perceived PBC is viewed as the perceived self-efficacy in performing a specific behaviour (Ajzen, 1991; Chandran & Aleidi, 2018), which is influenced by several factors. Of particular importance in this study is knowledge and its relationship with awareness. Thus far, the discussions on attitude formation (as influenced by personality) have outlined the process of subsidiation. In turn, subsidiation influences the formation of sentiments, which are learned and thus are based on knowledge acquisition (see Figure 4.2 in Chapter 4).

In this context, it is assumed that such knowledge acquisition takes place after reaching a heightened state of awareness relating to a specific issue. For example, a Facebook user is made aware of social media surveillance, and because they use Facebook, they can subsequently investigate how this surveillance affects them. New knowledge is acquired during the investigation, which leads to the creation of a sentiment and ultimately, an attitude adjustment towards social media surveillance. Of course, not all individuals may feel the need to acquire such knowledge as determined by what makes them unique. It is this influence, namely personality, which forms the core of this study.

Notwithstanding situations where certain Facebook users do not wish to learn more, the research model includes the construct *Information security awareness* as part of a cycle that influences knowledge acquisition. Here, it is important to note that neither knowledge nor awareness should be seen as a single-entry point into this cycle. If anything, it is the sentiment enriched attitude that is formed, which is of utmost importance. In this regard, the learning that takes place (part of creating a sentiment) could be attributed to either awareness or knowledge. From a theoretical perspective, this cyclical relationship is not only supported in the original TPB, but also within this study's research model. In the original version, an individual's assessment as to how effective one would be at performing a behaviour is also dependant on knowledge (Ham et al., 2015). However, other factors such as time, money, and other resources that influence self-efficacy are not of interest in this context. Unlike learning these resources are not cognitive and thus excluded from an individual's psyche. In turn, this makes the broader use of PBC (which does include such resources) unsuitable within the context of this study.

In the adapted version of the TPB (this study's research model) the relationship between attitude and awareness is bidirectional in nature. This not only supports the cyclical nature of this relationship, but also makes it possible for either awareness or attitude to influence the resultant process of knowledge acquisition. For example, an individual high in Openness to Experience may become aware of surveillance through some other means (i.e., significant others) and may wish to learn more, out of a sense of curiosity and in doing so, form or change an attitude. Conversely, an individual high in Conscientiousness may first explore all the nuances of a Facebook App (or Facebook in general) and through this learning, may become more aware.

Other researchers have also similarly adapted the TPB, by expanding their understanding of PBC, as opposed to the focused definition used in this study. For example, Ham et al. (2015) included the concept of locus of control as part of PBC in their study on *green food* adoption. Karimi et al. (2017) also argues that PBC should be viewed as a concept that includes control. Specifically, control over the intended behaviour and not necessarily the broader definition of control as explained by locus of control. In fact, Karimi et al. (2017)

regards locus of control as an individual difference modelling its influence on both PBC and attitude towards entrepreneurial intentions - a statistically significant influence in the context of their study.

Rhodes & Courneya (2003) discusses subdividing PBC by focusing on the concept of self-efficacy and controllability - specifically contemplating whether a behaviour is entirely within the control of an individual. Interestingly, and unlike Ham et al. (2015), Rhodes & Courneya (2003) argues that control should be viewed as a concept that stands apart from self-efficacy. Like Rhodes & Courneya (2003), Chandran & Aleidi (2018) adapted the TPB, but used perceived self-efficacy instead of PBC, rather than evaluating the influence of a broad range of resources including technological ones. The use of self-efficacy as an influence on intent is also used within Protection Motivation Theory (PMT). For example, Warkentin et al. (2016) used PMT to motivate that an increased awareness of self-efficacy will increase the intent to behave securely. As such, within the context of this study, awareness is understood as a broader concept - one that follows the act of perception.

In addition to awareness's relationship with self-efficacy and attitude, the TPB (and this study's model) also illustrates a bi-directional relationship with social norms. As such, in the context of this study, the very act of being influenced by norms also influences awareness - specifically as to what significant others do or think one should do. For example, a number of the items associated with the construct *Information security awareness* measure respondents' use of Facebook privacy settings. If a family member happens to make effective use of their privacy settings, this will most likely affect other family members to also use these settings. In doing so, other family members become aware of not only the use of these settings, but also why they are used. This social norm-based learning that takes place not only influence a Facebook user's level of awareness and attitude, but also allows this study's view of information security awareness to integrate with the TPB.

5.4.2 Behavioural influence of awareness

As with the other theoretical concepts discussed thus far, information security awareness also influences behaviour and is often not measured in terms of how individuals perceive and think about information security (Bartsch & Dienlin, 2016; Tsohou et al., 2015). To address this, authors have taken a variety of approaches to understand how information security awareness, knowledge, and perceptions influence each other. For example, Sundar et al. (2013) found that when participants were made aware as to how their personal information could be misused (via a video) their intention to disclose personal information was lower than those participants who were made aware of the benefits of disclosing personal information. Sundar et al. (2013) further argues that self-reported concerns about information privacy are the result of systematic processing, whereas actual behaviour is determined by heuristic means.

These decisions and resultant behaviour are further compounded by participants' inability to make informed privacy decisions. In this regard Hirschprung et al. (2016) found that when individuals lack the requisite knowledge or are not aware, they base decisions on speculation and do not think it through rationally. The more aware and knowledgeable an individual is, the more rational these decisions (and resultant behaviour) become. The latter statement is confirmed by van Schaik et al. (2018) who report that Facebook users who are more aware of information privacy concerns were generally satisfied with their privacy settings (i.e., visibility of their personal information). These findings also align with those of Miltgen & Peyrat-Guillard (2014) who did a similar privacy-based study amongst several European countries - albeit qualitatively. What these studies did not consider was the effect of being overly optimistic (i.e., optimism bias). For example, younger individuals incorrectly believed their information to be safer and more private than it actually was. Similarly, an increase in the awareness of information security threats has been found to have a significant positive influence on the strength of not only passwords (Mamonov & Benbunan-Fich, 2018), but also their composition (Saridakis et al., 2016).

Nevertheless, information security awareness could also influence the disclosure of personal information in unexpected ways. For example, Karwatzki et al. (2017) found that an excessive number of transparent features inhibit individuals from sharing personal information and raised concerns regarding the privacy of personal information. Similarly, some studies have found that an individual's personality influences how information security awareness concepts are internalised when undergoing information security awareness training (McCormac et al., 2017). It stands to reason that both knowledge and awareness not only influence information disclosure, but also individuals' privacy concerns (Parsons et al., 2017). In those instances where the aforementioned does not apply, individuals are not knowledgeable enough to protect their personal information and thus avoid secure behaviour (Bergström, 2015).

Thus far, the discussions have been focused on how the literature supports the influence of the primary constructs within this study's research model. It has also explained how to incorporate attitude, social norms, and awareness within the TPB. What it has not done is to theorise the context.

5.5 The surveillance of data in context

Much of the theory above is better understood by way of contextual examples - specifically those related to surveillance. This serves a dual purpose; it further contextualises the problem of this study and theorises how these have led to both the formation and change of user attitudes, the influence of norms and awareness of both government and social media surveillance. Since this study extends the TPB by substituting perceived behavioural control for the construct *Information security awareness*, it will use Edward Snowden as an example, simply because of the sudden and renewed awareness of data surveillance after his public announcements.

During the analysis of the articles identified in the first phase, a brief content analysis of several interviews and documentaries was performed as part of the process of backward searching. These ranged from interviews with:

- Michael Hayden (former CIA director) (Hayden, 2014),
- Edward Snowden (Snowden, 2013) as well as,
- Debates with privacy lobbyists, such as Glenn Greenwald (Hayden, 2014), and
- Documentaries.

From this analysis and Snowden's testimony (Snowden, 2013), it is clear that he changed his attitude towards not only government surveillance, but also information privacy in general. Further analysis revealed that several moral/ethical issues underpin government surveillance and information privacy. It is argued that specific decisions regarding the moral or ethical nature of government surveillance or similar situations are only possible post judgement. Hence, the applicability of judgement within the context of this thesis (see Figure 5.2) - specifically about attitude formation and change. As such, it is only by judging a situation or object that one can classify it as good, unnecessary, or required (keywords from questionnaire items 65-70). For example, given that the United States Patriot Act initially authorised the NSA to conduct dragnet-trait surveillance, is that good, required, or simply unnecessary? Even after President Bush ceased the collection of metadata (under the program *Stellar Wind*), it was replaced by the Foreign Intelligence Surveillance Act (FISA), based on a court judgement in the matter (Greenwald & Ackerman, 2013). These actions (both NSA's and Snowden's) are based on a set of contradictory beliefs. The NSA believes that government surveillance is conducted as a matter of national security, whereas Snowden believes that this is an abuse, perpetrated by the NSA. At its core, beliefs form part of an ideology (Van Dijk, 1998) which is fundamentally informed or shaped by the act of judging. Smith et al. (1998, p.88) is clear in this regard, stating that,

> *"...to make a judgement is the fundamental way to form a belief."*

This further substantiates the claim that once an individual perceives, these perceptions are judged, which in turn, influences the individuals' attitude - either positively or negatively. As such, both the NSA and Snowden base their beliefs about government surveillance on what is essentially a set of shared beliefs. Such ideological beliefs influence not only the actions of the NSA and Snowden, but also society at large, who either with or against Snowden, depending on their own beliefs and subsequent attitude towards government surveillance.

5.6 Summary

This chapter presented several discussions on the core aspects of this study's theoretical background. By way of a diagram, each construct of the Theory of Planned Behaviour was discussed by specifically indicating how it is integrated within the context of this study.

These discussions not only provided evidence as to the behavioural influence of these theoretical elements, but also indicated how they are aligned with the questionnaire items

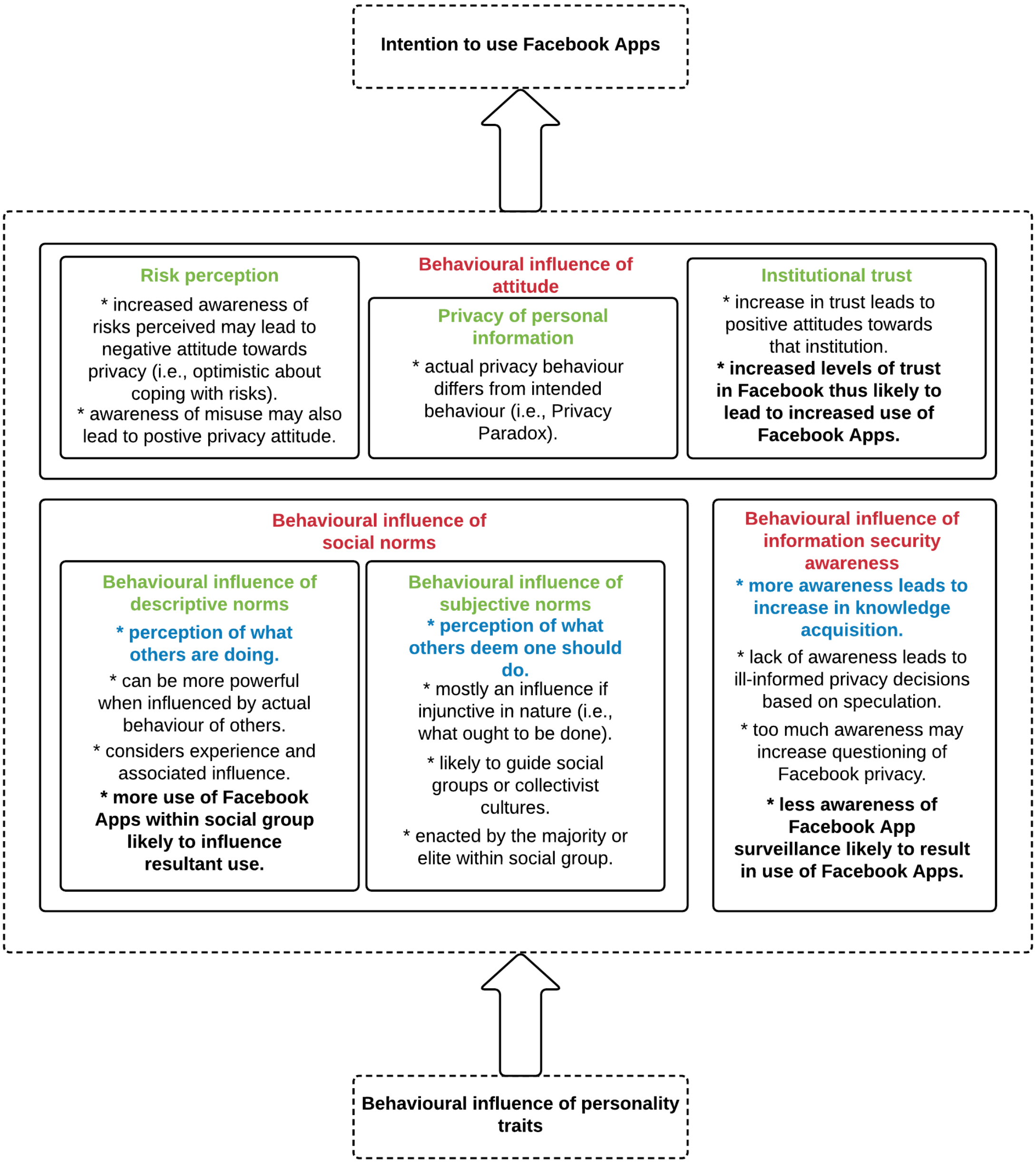

Intention to use Facebook Apps
Behavioural influence of attitude
Risk perception
* increased awareness of risks perceived may lead to negative attitude towards privacy (i.e., optimistic about coping with risks).
* awareness of misuse may also lead to postive privacy attitude.
Privacy of personal information
* actual privacy behaviour differs from intended behaviour (i.e., Privacy Paradox).
Institutional trust
* increase in trust leads to positive attitudes towards that institution.
* increased levels of trust in Facebook thus likely to lead to increased use of Facebook Apps.
Behavioural influence of social norms
Behavioural influence of descriptive norms
* perception of what others are doing.
* can be more powerful when influenced by actual behaviour of others.
* considers experience and associated influence.
* more use of Facebook Apps within social group likely to influence resultant use.
Behavioural influence of subjective norms
* perception of what others deem one should do.
* mostly an influence if injunctive in nature (i.e., what ought to be done).
* likely to guide social groups or collectivist cultures.
* enacted by the majority or elite within social group.
Behavioural influence of information security awareness
* more awareness leads to increase in knowledge acquisition.
* lack of awareness leads to ill-informed privacy decisions based on speculation.
* too much awareness may increase questioning of Facebook privacy.
* less awareness of Facebook App surveillance likely to result in use of Facebook Apps.
Behavioural influence of personality traits

Figure 5.5: Summary of the core behavioural influences reviewed in this chapter

used to measure the aspects of this study. Throughout, the chapter also argued the importance of an individual's perceptions and the beliefs formed as a function of judgement as influenced by their ideological worldviews. The chapter concludes with a contextual example illustrating the influence of attitude, beliefs, and judgement. The next chapter provides an outline of this study's research model and propositions by way of brief discussions on the behavioural influence of attitude, social norms, awareness, and personality.

Chapter 6

RESEARCH MODEL AND PROPOSITIONS

> "In spite of everything I shall rise again: I will take up my pencil, which I have forsaken in my great discouragement, and I will go on with my drawing."
>
> — Vincent van Gogh

This chapter provides an overview of research models and theories. It starts with a review of other theories used within the field of Behavioural Information Security (BIS) all the while motivating in favour of this study's research model. This motivation not only formally presents the propositions, but also visually illustrates them in Figure 6.1 - an adapted version of the Theory of Planned Behaviour (TPB). Importantly, this chapter makes it clear as to how this study contributes theoretically.

6.1 Typical information security research

In this study, an adapted version of the TPB is used as a theoretical foundation, to guide both the development of the research instrument constructs and the resultant research model. It is, however, not the only theoretical means of studying BIS. As such, the following subsection also discusses the use of other theories. This applies specifically to those theories that have been used to evaluate the influence of personality within the field of BIS.

6.1.1 Use of theory

Not all the theories and resultant research models reviewed in this study are directly related to BIS. Additionally, some of these studies do not situate their empirical work within social media. They are useful, however, to illustrate how known theories have been adapted to evaluate (and incorporate) similar psychological aspects, as well as their resultant influence on BIS concepts. For example, Bulgurcu et al. (2010) combined the TPB and Rational Choice Theory (RCT) to explore employee's attitude towards complying with information security policy. Within the context of the latter study, RCT contains constructs to understand how individuals decide whether or not to enact a behaviour. These constructs are subsequently grouped into those that determine beliefs (related to outcomes) and those that determine the assessment of consequences.

Chakraborty et al. (2013) on the other hand, combined Social Capital Theory (SCT) with the Activity Theory of Ageing (ATA) to explain how the process of getting older not only increases these individual's use of social media, but also subjectively influences other older users to share personal information (as a result of increased usage). Some social media-based studies have also employed theories such as Uses and Gratification Theory, which aims to understand the trade-off between what is gained from using social media, as opposed to the risk (misuse of information) in doing so. Understanding the influence of threats has also featured in several BIS studies (Hanus & Wu, 2016; Herath & Rao, 2009b; Tsai et al., 2016). In these instances, Protection Motivation Theory (PMT) is used and posits that an individual's appraisal of threats, and how to cope with those threats, influences behavioural intent. Similar to Bulgurcu et al. (2010), Vance et al. (2012) also explored information security compliance, but did so by integrating habit with PMT. Conversely, Thompson et al. (2017) made use of PMT to explore home users' intention to adopt secure behaviour - specifically related to personal computing devices (mobile phones, for example).

To better understand the willingness of individuals to disclose personal information as part of Internet transactions, Dinev & Hart (2006) combined intent from the TPB with Privacy Calculus. Here, Dinev & Hart (2006)'s use of Privacy Calculus focused on those decision-making processes that influence individuals' intent to disclose personal information based on their perceptions about information privacy. For example, if an individual decides to conduct an Internet-based transaction does the benefit of this outweigh the risks of doing so? In a more recent article Hirschprung et al. (2016) made use of Prospect Theory to explore a similar relationship between an increase in the probability that personal information will be disclosed based on the cost of doing so.

Although some of the theories mentioned above provide adequate support to evaluate information privacy, attitude, and behavioural intent, they do not necessarily incorporate social norms. Those studies that do evaluate the influence of social norms do so using different descriptions, such as *social influence or social sanctions* (Herath & Rao, 2009a; Johnston & Warkentin, 2010; Siponen & Vance, 2010) or they evaluate the constituent elements of social norms (subjective, descriptive or injunctive norms) separately (Ifinedo, 2014; Safa et al., 2017). Recent studies that do evaluate it as a single construct, either use it within different disciplines (Emami & Khajeheian, 2019; Esfandiar et al., 2019; Wang, 2019) or they combine it with only certain social norms (D'Arcy & Lowry, 2019; Grimes & Marquardson, 2019; Merhi & Ahluwalia, 2019).

To study awareness of other users and their privacy concerns, Lowry et al. (2011) makes use of Social Exchange Theory and combines it with the Theory of Reasoned Action (TRA), but only makes use of attitude. These authors also explicitly argue in favour of actual self-disclosure as opposed to intent. In fact, similar to the concept of social norms, few studies have explored information security awareness by adapting the TPB, as this study has done. Those that do, either theoretically explore information security awareness (Tsohou et al., 2015) within the context of the TPB, but exclude social norms (Hajli & Lin, 2016; Safa et al., 2015) or both attitude and social norms (Humaidi & Balakrishnan, 2015). Those that do use all of the latter constructs fail to include some (McCormac et al., 2017) or all of the Big Five personality traits (Flores & Ekstedt, 2016). It thus stands to reason that the use of the constructs contained in this study's research model provides a means to contribute to BIS from a theoretical point of view.

6.2 Theory development and propositions

In addition to the literature reviewed in Chapters 4 and 5, this section provides a series of focused discussions that not only define the research model constructs, but also formally states the propositions they are associated with. Note that these propositions are not only based on the brief literature that precedes them here, but also on the preceding literature chapters. As such, both the research model (constructs and relationships) and the propositions are primarily derived from the literature review (i.e., Chapters 4 and 5). Furthermore, note that all the research model constructs were classified as reflective in nature (Gefen et al., 2000; Petter et al., 2007)

6.2.1 Intention to use Facebook Apps

This construct consists of a single item (item 14 in Appendix A), which evaluates how likely respondents are to continue their use of Facebook Apps. This question is deliberately placed towards the start of the questionnaire so as to capture a more true reflection of respondents' intention in this regard. In other words, a response not marred by the items to follow. For example, many of the awareness items will likely increase the likelihood that a respondent may avoid Facebook Apps. Importantly, this is the dependent construct in this study.

6.2.2 Attitude towards privacy

Within the context of this study, attitude is defined as an individual's propensity to either positively or negatively evaluate another individual, situation, or object (Ajzen, 2005, p.3). As such, specific individuals may hold a positive or negative attitude towards Facebook App surveillance for any number of reasons. One such reason might be related to the influence of their personality; specifically the influence of the Big Five personality traits, which are illustrated on the far left in this study's research model (see Figure 6.1).

However, irrespective of such influences, an individual's attitude alone also drives their intention to enact certain behaviour (Kim & Hunter, 1993). In this study, the items associated with the construct *Attitude towards privacy* measure an individual's attitude - specifically, their attitude towards the misuse of their personal information while making use of Facebook Apps. Thus, if an individual forms (or have already formed) a negative attitude towards privacy, this study posits that they may be less inclined to use Facebook Apps. In this regard, the literature provides several instances to support the behavioural influence of attitude. For example, Jayawardhena (2004) found that an individual's attitude towards online shopping directly predicts their intention to enact such forms of shopping. Consumer

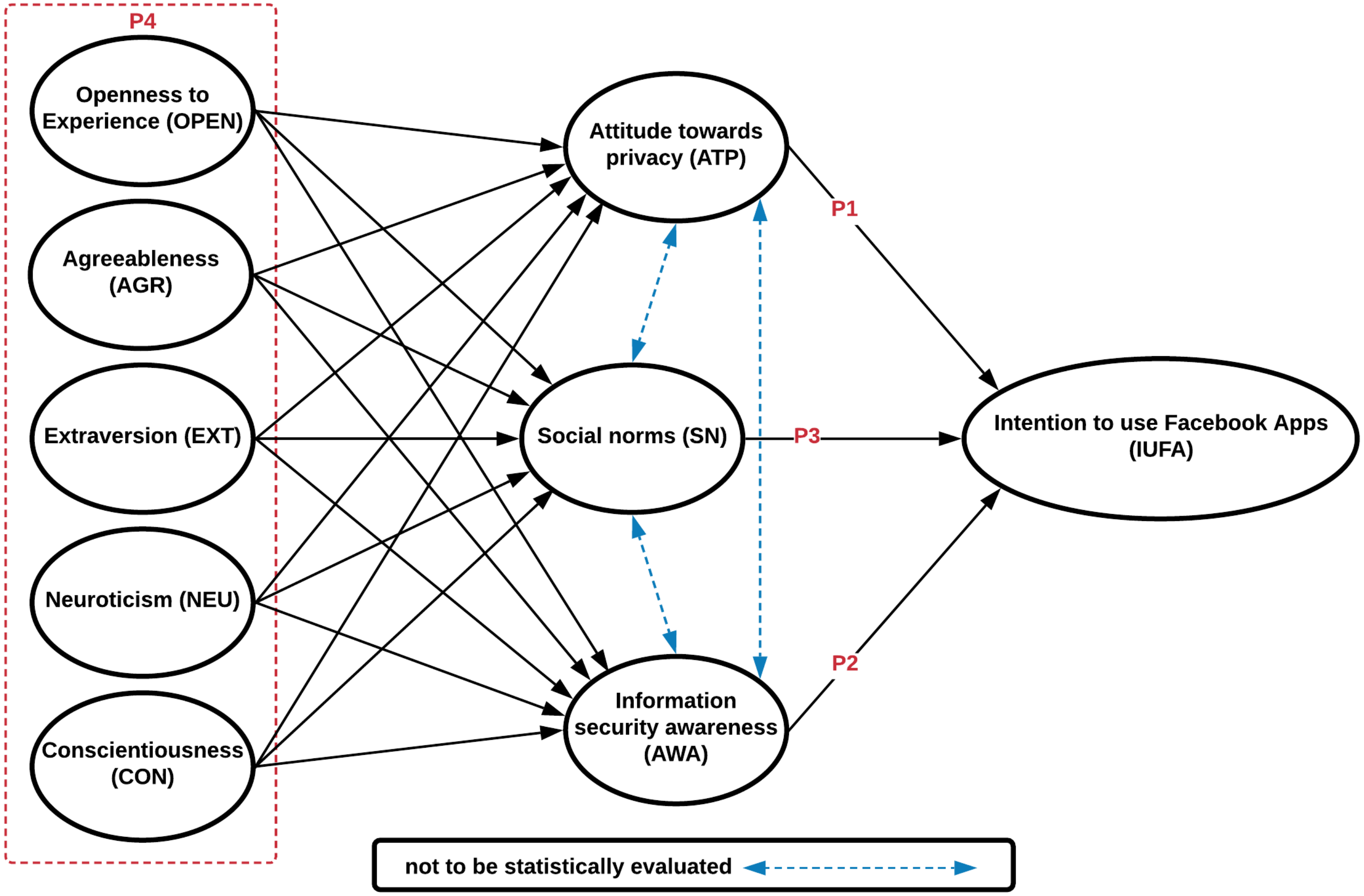

P4
Openness to Experience (OPEN)
Agreeableness (AGR)
Extraversion (EXT)
Neuroticism (NEU)
Conscientiousness (CON)
Attitude towards privacy (ATP)
Social norms (SN)
Information security awareness (AWA)
P1
P3
P2
Intention to use Facebook Apps (IUFA)
not to be statistically evaluated

Figure 6.1: This study's research model in propositional form

behaviour studies - specifically those related to the purchase of organic food - have also found that positive attitudes towards such food increase an individual's intention to purchase *green food* (Basha et al., 2015). Similarly, Nguyen et al. (2016) found that consumers who exhibit a positive attitude towards environmental protection also tended to purchase environmentally friendly appliances. Further evidence of the broad behavioural influence of attitude is provided by Venkatesh & Morris (2000) where the authors investigate how gender and social norms (among others) influence the adoption and resultant use of technology.

More support within the context of this study can be found within the field of Behavioural Information Security (BIS). For example, Haeussinger & Kranz (2013) found that both information security awareness and attitude has a direct and positive influence on the intention of information security professionals to enact secure behaviour. Related findings are reported by Blythe et al. (2015) where the authors confirm the behavioural influence attitude has on the intention of employees to comply with information security policies - albeit qualitatively. Amankwa et al. (2018) also found that attitude displayed the most significant effect size on complying with information security policies. For example, a positive attitude towards security compliance correlated directly with enacting related security behaviour. This confirms the results of earlier studies, which also found a strong correlation between attitude and the intention to adopt secure behaviour in general, and information security policies in particular (Hazari et al., 2008; Lee & Kozar, 2005).

Although the latter studies are empirically situated within organisations, the same behavioural influence of attitude also applies to social media. For example, there are several studies that have investigated the disclosure of personal information on these platforms (Chang & Chen, 2014; Hallam & Zanella, 2017; Hirschprung et al., 2016). It is worth noting that disclosing personal information on social media is viewed similarly to an individual who installs or uses a Facebook App. In this instance, the App does not necessarily disclose the personal information directly to other members of the social media platform, but rather collects it to be disclosed in some other way or form at a later stage. For example, Chen & Sharma (2015) found that a Facebook user's attitude directly influences their intention to disclose personal information. This was found to be particularly significant where Facebook users exhibited positive attitudes towards information disclosure on social media. In such instances, individuals also tended to increase their use of Facebook, which further increased the amount of personal information being disclosed. Koohikamali et al. (2017) also found a statistically significant relationship between attitude and the intention to disclose personal information - albeit the personal information of others (i.e., Facebook friends for example). Given the aforementioned behavioural influence of attitude, it is thus plausible that a Facebook user's attitude towards information privacy (shortened to privacy as the official label of the construct) will also influence their intention to use Facebook Apps. It thus stands to reason that:

Proposition 1. *An individual's attitude towards privacy will influence their intention to use Facebook Apps.*

This proposition corresponds to the relationship between the construct *Attitude towards privacy* and *Intention to use Facebook Apps*, which is visually depicted by the label **P1** in Figure 6.1. Importantly, it is measured by the seven items associated with the construct *Attitude towards privacy* (see Appendix A).

6.2.3 Information security awareness

The inclusion of awareness in this manner forms one of the core aspects of this study's theoretical contribution. It not only replaces Perceived Behavioural Control (PBC), which features in the original version of the TPB, but also plays a prominent role within the cycle of knowledge acquisition. This is crucial in that it allows for the integration of awareness and attitude formation based on the influence of personality (as per subsidiation in Chapter 4). As such, this study does not make use of a single and strict theoretical definition of awareness. Instead, awareness is viewed as a broad term that incorporates an individual's perceptions regarding the security of their personal information; hence, the inclusion of items that measure an individual's level of concern regarding the use and safekeeping (via privacy settings) of their personal information. In this regard, it is understood that an individual's level of awareness influences their level of concern for the safety of their personal information.

Several studies have found it pertinent also to study this relationship. For example, Hansla et al. (2008) investigated individual beliefs on the consequences of awareness on environmental concerns and found that awareness of consequences was significantly related to environmental concerns. Similarly Fornara et al. (2016), found that awareness of consequences is significantly related to an individual's attitude towards the use of renewable energy. Moreira et al. (2017) found that the relationship between awareness and behaviour also applies to consumers - precisely their intention to purchase based on brand awareness and experience. In a related consumer-based study Duffett (2015) found that South African Facebook users' intention to make purchases online is influenced by platform-based awareness campaigns surrounding specific products (i.e., via advertising, for example).

Additionally, the behavioural influence of awareness also applies within the field of behavioural information security. For example, Flores & Ekstedt (2016) found that information security awareness is positively related to self-efficacy and individuals' attitude towards resisting social engineering attacks. Similarly, Bauer et al. (2017) argues that the more aware individuals become (via awareness campaigns), the more likely they are to adhere to information security policies. Other studies that also argue in favour of the relationship between knowledge and awareness (Safa et al., 2016; Safa & Von Solms, 2016) have also found that a heightened state of awareness positively influences an individual's attitude and intention to comply with security policies. Additionally, awareness also significantly affects how individuals perceive threats (Hanus & Wu, 2016). In turn, such perceptions influence security appraisal processes, which ultimately determine if and to what extent individuals adopt secure behaviour.

Related social media-based studies have also reported similar findings. For example, Benson et al. (2015) found that social media users are inclined to disclose less personal information when perceived to have more control over said information. Conversely, awareness as to how the platform uses personal information increased users' intention to disclose personal information. Even though the secondary use of personal information by social media platforms is likely to impact on the privacy of said information. The findings of Zlatolas et al. (2015) contradict those of Benson et al. (2015) who found that privacy-aware Facebook users are less inclined to disclose personal information. Given that the use of Facebook Apps results in the reduction of the privacy of personal information, it is thus plausible that an individual's awareness of Facebook App surveillance will also influence these individuals' intention to use Facebook Apps. As such, it stands to reason that:

Proposition 2. *An individual's information security awareness of Facebook App surveillance will influence their intention to use Facebook Apps.*

This proposition corresponds to the relationship between the construct *Information security awareness* and *Intention to use Facebook Apps*. It is depicted by the label **P2** in Figure 6.1 and measured by the 12 items associated with the construct *Information security awareness* (see Appendix A).

6.2.4 Social norms

Given the importance of social norms within social media (Haynes et al., 2016), this study provides a measure of subjective and descriptive norms - another component of this study's theoretical contribution. As discussed in Chapter 4, social norms is used as an umbrella term, to group together both descriptive and subjective norms. Using social norms in this manner is not only supported from a theoretical perspective (Cialdini et al., 1990; Fishbein & Yzer, 2003; Lapinski & Rimal, 2005), but also empirically (see examples below). Although several studies measured the influence of subjective or descriptive norms, individuals often misunderstand the subtle differences between behaviour that is prescribed (subjective norm) as opposed to described. Hence the measurement of both subjective and descriptive norms.

Several studies similarly used social norms in their studies - albeit within different disciplines and contexts. For example, Zlatolas et al. (2015) made use of social norms by integrating them into Communication Privacy Management theory. The results of their study indicated that the more aware a user becomes (due to social influence of friends), the less information is disclosed. In a study on information security policy compliance, Herath & Rao (2009b) found that both subjective and descriptive norms significantly influence an individual's intention to comply with security policies.

As opposed to referring to social norms, some studies also use the description personal norms, depending on whether or not an individual has internalised the social norms in question. For example, Yazdanmehr & Wang (2016) conceptually divided personal norms into subjective, descriptive, and injunctive norms to evaluate their influence individually. Here, results indicated that as a whole, personal norms significantly influence an individual's intention to comply with information security policy. Similar results are reported by Cuganesan et al. (2018) where the authors investigated the influence of several formal controls on norms in addition to attitude and self-efficacy. From a social media perspective Vickery (2015) found that social norms influence not only the information being disclosed, but also on which platform it is to be disclosed. Nevertheless, participants agreed on the behavioural influence of social norms across both Twitter and Facebook.

Another recent study on the influence of information privacy concerns within the sharing economy, found that social influence exhibits a significant positive relationship with an individual's intention to share. The more emphasis is placed on norm-based sharing within a social group or community, the more these norms influence an individual's intention to share personal information (Lutz et al., 2018). In addition to the influence of social norms on information disclosure, other studies have also explored the relationship between social norms and technology adoption. For example, Mamonov & Benbunan-Fich (2017) found that social norms negatively influence the adoption and subsequent use of the Facebook Gifts service. In this regard, the perceived low effort required to make use of the gifting service counters the accepted social norm, which requires a gift-giver to invest enough effort to locate a suitable gift in person (i.e., not just merely giving a convenient electronic Facebook gift).

As such, if an individual's family deems it inappropriate to play Facebook games (also a type of App), he or she may avoid using such Apps. Conversely, if an individual's peer group are passionate about music and regularly use Spotify (using their Facebook credentials), he or she may enact similar behaviour. Given the latter, this study thus proposes that:

Proposition 3. *Social norms will influence an individual's intention to use Facebook Apps.*

This proposition corresponds to the relationship between the construct *Social norms* and *Intention to use Facebook Apps*. It is depicted by the label **P3** in Figure 6.1 and measured by the seven items associated with the construct *Social norms* (see Appendix A).

6.2.5 Big Five personality traits

Because of its psychological nature, personality is well suited to behavioural information security studies (Ajzen, 2005). For example, Dickason & Ferreira (2018) recently studied the influence of personality on South African investors - specifically concerning their financial biases and tolerance for risk. Using the Domain-specific risk-taking scale (Dospert) to measure investor personalities, the authors conclude that conservative investors' (a Dospert personality trait) trading behaviour exposes them to higher levels of risk, since they tend to hold on to poor investments. Additionally, moderate personalities were subject to investment behaviours such as regret aversion, due in part due to their propensity to make investment decisions based on past mistakes.

Additional support for the behavioural influence of personality is found in a study focused on adolescent bullying (Kelly et al., 2018). Of the four personality traits measured (*anxiety sensitivity*, *hopelessness*, *impulsivity* and *sensation seeking*) it was found that adolescents with high levels of impulsivity are more likely to bully. Conversely, those adolescents high in hopelessness were found to be likely victims of bullying behaviour.

Studies using the Big Five have also found support for the behavioural influence of personality. For example, Camadan et al. (2018) found that teachers high in Openness to Experience and Extraversion are more likely to adopt new classroom technologies. This stands in contrast to those teachers high in Neuroticism and Agreeableness who were found less likely to adopt new classroom technologies. Over and above the diverse contexts mentioned thus far, several behavioural information security studies have also argued the behavioural influence of personality (McCormac et al., 2017; Shropshire et al., 2015; Warkentin et al., 2012; Williams et al., 2017). Specific examples include a study conducted to explore both the dispositional and situational factors that influence information security compliance behaviour (Johnston et al., 2016).

In the latter study, the authors divided the Big Five traits into two groups - Conscientiousness, Agreeableness, and Neuroticism were modelled as stability meta traits with Openness to Experience and Extraversion forming part of plasticity traits. Here, the findings suggest that individuals high in the stability meta-trait are more sensitive to threat vulnerability and severity as well as the certainty of sanctions. It stands to reason that these individuals are less likely to violate information security policies. Conversely, individuals high in the plasticity meta-trait are more likely to commit security policy violations. This amidst perceptions indicative of high response efficacy as well as certainty of sanctions. Additional support for personality's behavioural influence also extends to social media. For example, Wallace et al. (2017) found that individuals high in Conscientiousness, Extraversion, and Agreeableness are less likely to experience Facebook-situated envy. Here, Facebook-situated envy is defined as envious comments directed towards other individuals based on their comments, which imply superiority. Conversely, individuals high in Neuroticism are more likely to experience such forms of envy, which implies them posting comments interpreted as superior. As such, the perceptions and associated behaviour of certain social media users are likely to differ based on their personality. It thus stands to reason that:

Proposition 4. *An individual's personality will influence their intention to use Facebook Apps.*

This proposition is represented by all the uni-directional relationships illustrated between the five personality constructs (the traits of the Big Five) and the constructs *Attitude towards privacy*, *Social norms* and *Information security awareness*. The 44 item Big Five Inventory (BFI) measures the personality of the respondents (John & Srivastava, 1999). Note that the BFI has proven to be not only valid and reliable, but also an established measure within the field of behavioural information security.

6.2.6 Social desirability

This study also made use of a social desirability scale to ascertain to what extent a respondent is *faking good* or *faking bad*. Often employed within psychological studies, social desirability scales are also used within behavioural information security studies - specifically those focused on awareness (McCormac et al., 2017; Pattinson et al., 2017). Using social desirability scales in this manner enables behavioural studies to gain additional insight as to which responses are subject to faking as described above. For example, Parsons et al. (2017) used the same shortened Marlowe-Crowne variant as this study (8 items as per Appendix A) and found that respondents provided overly positive answers when asked about security incident response as part of a larger information security awareness initiative. Related studies, such as those conducted by Snyman et al. (2017); Snyman & Kruger (2017), use behavioural threshold items to measure an individual's behavioural intention. Note that the use of behavioural thresholds only applies in research settings where the respondents either know each other or know of each other. It thus stands to reason that such a behavioural threshold approach will not work within the context of this study, since the data is collected via Amazon Mechanical Turk.

6.2.7 Demography

Additionally, certain demographic aspects are also measured. These include respondents' age, gender, level of education, and level of Facebook use. In total, 13 items are used to measure the demography of this study (see Appendix A for a complete list).

6.3 Summary

This chapter provided a discussion around both the general use of behavioural information security theories and motivation for the use of the TPB within the context of this study. After illustrating a propositional version of this study's research model, additional support for each of the four propositions was provided followed by a formal statement of each proposition. Together, the discussions above allow for the articulation of this study's theoretical foundation by illustrating the unique combination in which the research model constructs have been used. In the following chapter, a detailed outline of this study's results are provided.

Chapter 7

RESULTS

> "Recommend virtue to your children; it alone, not money, can make them happy. I speak from experience."
>
> — Ludwig von Beethoven

This chapter builds on the previous chapters by presenting the results of the statistical analyses. The results of the questionnaire's validity and reliability tests (both the pilot and final questionnaire) are presented, followed by the outcome of the data collection process. Additionally, the study's descriptive statistics (univariate analyses) are presented with additional inferential results pertaining to the multivariate analysis. From the latter multivariate analysis both a measurement and structural model was developed. The chapter concludes by discussing the structural model's results within the context of this study's propositions.

7.1 Results of the pilot study

The following sections contain the results of the pilot study conducted using Amazon Mechanical Turk (AMT).

7.1.1 Data collection

Data collection for the pilot study was conducted from the 9th of December 2018 to the 11th of December 2018. During this time, a total of 21 responses (N=21) were collected. All of these responses were deemed suitable and thus used in the pilot study. Suitability was determined based on the following criteria:

- The response had to be complete (i.e., all questions answered), and
- Their social desirability scores had to be equal to or lower than 20.

7.1.2 Univariate analysis

Several demographic questions were asked at the beginning of the pilot questionnaire. From an age perspective, 42.9% of the respondents were between the ages of 25-34 (inclusive) making it the largest age group in the sample. Additionally, up to 95% of the respondents were 54 years of age or younger. See Table 7.1 for the age distribution of all the respondents.

Table 7.1: Age distribution of respondents

Age groups	**Frequency**	**Percent**	**Cumulative percent**
18 to 24	1	4.7%	4.7%
25 to 34	9	42.9%	47.6%
35 to 44	8	38.1%	85.7%
45 to 54	2	9.5%	95.2%
55 to 64	1	4.8%	100.0%

The sample contained more males than females, as presented in Table 7.2

Table 7.2: Gender distribution of respondents

Gender	**Frequency**	**Percent**	**Cumulative percent**
Female	9	42.9%	42.9%
Male	12	57.1%	100.0%

Respondents were also asked about the highest level of education they have achieved with more than half (52.4%) of the respondents having obtained a Bachelor's or equivalent degree (see Table 7.3).

To understand how respondents use Facebook, this study also measured both general use (in minutes per day), the number of friends and the number of Facebook Apps used. Together, these aspects rounded off the demographic items of the pilot study. As per Table

Table 7.3: Distribution of respondents' level of education

Level of education	Frequency	Percent	Cumulative percent
No degree or up to high school	8	38.1%	38.1%
Bachelors degree or equivalent	11	52.4%	90.5%
Masters degree and above	2	9.5%	100.0%

7.4, 47.6% of the respondents reported having more than 200 Facebook friends. The distribution of Facebook users' friends displays bi-modal properties with two distinct peaks - one at 19% (151-200 friends) and another at 23.8% (more than 400).

Table 7.4: Distribution of number of Facebook friends

No. of friends	Frequency	Percent	Cumulative percent
10 or less	2	9.5%	9.5%
11-50	2	9.6%	19.1%
51-100	0	0.0	0.0
101-150	3	14.3%	33.3%
151-200	4	19.0%	52.4%
201-250	2	9.5%	61.9%
251-300	2	9.5%	71.4%
301-400	1	4.8%	76.2%
more than 400	5	23.8%	100.0%

From Table 7.5 it is evident that 61.9% of respondents spend less than 31 minutes on Facebook per day with 4.8% spending up to 3 hours on Facebook per day.

Table 7.5: Distribution of time spent on Facebook

Minutes on Facebook	Frequency	Percent	Cumulative percent
less than 10 minutes	7	33.3%	33.3%
10-30 minutes	6	28.6%	61.9%
31-60 minutes	4	19.0%	81.0%
1-2 hours	3	14.3%	95.2%
2-3 hours	1	4.8%	100.0%

Since this study's focus is on the intended use of Facebook Apps, the pilot questionnaire included an item to investigate how many Facebook Apps respondents actually use. Interestingly, 9.5% of the respondents were not aware of how many Facebook Apps they use.

Similar to the data presented in Table 7.4, the distribution corresponding to the number of Facebook Apps used, is also bi-modal, with a peak at 33.3% (1-2 Apps) and 14.3% (more than nine Apps).

Table 7.6: Distribution of number of Facebook Apps used

No. of Facebook Apps	**Frequency**	**Percent**	**Cumulative percent**
1-2	7	33.3%	33.3%
3-4	4	19.0%	52.4%
5-6	4	19.0%	71.4%
7-8	1	4.8%	76.2%
more than 9	3	14.3%	95.5%
unknown	2	9.5%	100.0%

7.1.3 Validity and reliability testing

Once the pilot data was collected, tests for validity and reliability were conducted. Reliability is concerned with the extent to which an experiment, test, or any measuring procedure yields the same results on repeated measures. In this regard, Cronbach's alpha (CA) was used to check construct reliability (Bland & Altman, 1997; Cronbach, 1951). Cronbach's alpha values above 0.70 were deemed reliable.

Even though the personality items (Big Five Inventory) is significant in this study, other scales are also present and were also tested. Where possible, a CA value derived from the literature is included (as indicated by column *CA of lit* in Table 7.7). Note that some of the scales were constructed from various sources and as such do not have an associated literature-based alpha value in the column named *CA of lit*. The column named *CA* represents the alpha values obtained in the reliability tests of this study.

Overall, the alpha values obtained in the reliability tests of the pilot questionnaire were indicative of a reliable questionnaire except for the *Facebook and PC experience* scale. Nevertheless, it was included in the final questionnaire in the hope that larger sample size will increase the CA value. A summary of the reliability values associated with the pilot questionnaire scales is presented in Table 7.7.

The pilot questionnaire was also tested for validity. Validity can be defined as the extent to which any measuring instrument (such as a questionnaire) measures what it intends

Table 7.7: Results of the pilot questionnaire's reliability tests

Constructs	CA of lit	CA	Outcome
Facebook usage	0.830	0.930	Reliable
Facebook and PC experience	n/a	0.670	Not Reliable
Extraversion	0.880	0.930	Reliable
Agreeableness	0.790	0.880	Reliable
Conscientiousness	0.820	0.890	Reliable
Neuroticism	0.840	0.960	Reliable
Openness to Experience	0.810	0.900	Reliable
Social desirability	0.770	0.920	Reliable
Attitude towards privacy	n/a	0.880	Reliable
Social norms	n/a	0.850	Reliable
Information security awareness	n/a	0.870	Reliable

to measure. Two approaches were used to test for validity. Firstly, Principal Component Analysis (PCA) was used to ascertain which items are highly correlated across all the constructs (Cattell, 1966; Kaiser, 1974).

However, after conducting these initial validity tests, some inconsistencies were detected. For example, some of the items associated with the Agreeableness construct loaded incorrectly into Conscientiousness. The same applied to some of the items associated with Conscientiousness, which loaded in both Neuroticism and Agreeableness. Thus, additional validity testing was conducted. As such, an alternate approach to validity testing was used; namely, Pearson Product Moment Correlations (Altman & Bland, 2005). This second approach tested the correlations between the total construct score and the individual items that constitute these personality constructs. Items with non-statistically significant, very low coefficients (below 0.30) or negative coefficients were considered non-compatible with that sub-scale. The results of running this test on all five personality constructs are listed in Tables 7.8 through 7.12. Note that the numbers within the top row of these tables represent the item number occupied in the pilot questionnaire. Overall, these tables indicate that all the coefficients are positive, statistically significant, and above the threshold of 0.30 - therefore valid.

The following amendments were made to the pilot questionnaire:

- The pre-amble was shortened,

Table 7.8: Second validity test for *Extraversion*

Tests	18	23	28	34	39	44	49	54
Pearson Correlation	0.865**	0.883**	0.728**	0.820**	0.656**	0.801**	0.890**	0.910**
Significance (2-tail)	0.000	0.000	0.000	0.000	0.001	0.000	0.000	0.000

** = p<0.01

- Renaming and creating additional questionnaire pages to aid analysis. For example, the pilot questionnaire initially placed the items related to the construct *Attitude towards privacy* and *Social norms* on one page. In the final questionnaire these were placed on separate pages,
- Removing one of the demographic items related to the employment sector of respondents,
- Removing one of the items associated with the construct *Social norms* which did not load, and
- Re-shuffling the sequence of the questionnaire items. For example, the social desirability items were moved to the end of the questionnaire.

Following the latter changes, the questionnaire was used in the final study.

7.2 Results of the final study

The following sections contain the results of the final study, which also used Amazon Mechanical Turk (AMT) for its data collection.

7.2.1 Data collection

The process of data collection took place between the 24th of January 2019 and the 22nd of February 2019. Although this process resulted in the collection of 651 responses (N=651), several of these responses were deemed unsuitable. Suitability was determined based on the following criteria:

Table 7.9: Results of the second validity test for *Agreeableness*

Tests	**19**	**24**	**29**	**35**	**40**	**45**	**50**	**55**	**60**
Pearson Correlation	0.861**	0.630**	0.751**	0.681**	0.468*	0.771**	0.725**	0.780**	0.798**
Significance (2-tail)	0.000	0.002	0.000	0.001	0.033	0.000	0.000	0.000	0.000

** = p<0.01,
* = p<0.05

Table 7.10: Results of the second validity test for *Conscientiousness*

Tests	**20**	**25**	**30**	**36**	**41**	**46**	**51**	**56**	**61**
Pearson Correlation	0.665**	0.785**	0.641**	0.838**	0.817**	0.771**	0.639**	0.758**	0.748**
Significance (2-tail)	0.001	0.000	0.002	0.001	0.033	0.000	0.002	0.000	0.000

** = p<0.01

Table 7.11: Results of the second validity test for *Neuroticism*

Tests	**21**	**26**	**31**	**37**	**42**	**47**	**52**	**57**
Pearson Correlation	0.845**	0.907**	0.840**	0.939**	0.892**	0.822**	0.888**	0.938**
Significance (2-tail)	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000

** = p<0.01

Table 7.12: Results of the second validity test for *Openness to Experience*

Tests	**22**	**27**	**32**	**38**	**43**	**48**	**53**	**58**	**59**	**62**
Pearson Correlation	0.854**	0.688**	0.787**	0.652**	0.887**	0.755**	0.478*	0.933**	0.873*	0.690**
Significance (2-tail)	0.000	0.001	0.000	0.001	0.000	0.000	0.028	0.000	0.000	0.001

** = p<0.01,
* = p<0.05

- The response had to be complete (i.e., all questions answered),

- Both *attention trap questions* (see Appendix A) of the response had to be correctly answered. The use of these trap questions are encouraged to better filter unsuitable responses. For example, both the attention trap questions in this study asked respondents to solve a trivial mathematical equation. If they rushed to complete the questionnaire (i.e., clicked random response anchors), it would be easier to spot, because the equation's answer was most likely incorrectly answered. Hence, the response was discarded.

- The responses completed in less than five minutes were also discarded. This cut-off point was determined by averaging the completion times of all the responses. As such, the pilot study was not used in this regard.

- Their social desirability scores had to be equal to or lower than 20. No outliers were observed in this regard. As such, the social desirability construct was left out of the multivariate analysis, since it was unlikely that it would be able to indicate which responses needed to be excluded.

After applying the filter criteria, 537 usable responses (N=537) remained. These responses formed the basis of the subsequent process of multivariate analysis, which exceeded the required 385 to achieve statistical significance at the 95% confidence interval.

7.2.2 Univariate analysis

As part of the final study's univariate (descriptive) analysis both the demography and means of the constructs (and distributions) were analysed. After analysis of the histograms it was clear that some of the constructs were not normally distributed, thus favouring the use of Partial Least Squares (PLS) path modelling.

7.2.2.1 Demography

As in the pilot study, the final study's questionnaire included the same demographic items. In Table 7.13, the age distribution of the sample is presented with 73.7% of the respondents being less than 45 years of age. Additionally, the majority (40.0%) of the final study's respondents fall into the 25-34 age group.

Table 7.13: Age distribution of respondents

Age groups	Frequency	Percent	Cumulative percent
18 to 24	33	6.1%	6.1%
25 to 34	215	40.0%	46.2%
35 to 44	148	27.6%	73.7%
45 to 54	78	14.5%	88.3%
55 to 64	47	8.8%	97.0%
65 to 74	16	3.0%	100.0%

More female respondents completed the questionnaire (see Table 7.14), with the largest portion of the sample's respondents having obtained at least a bachelor's or equivalent degree (see Table 7.15).

Table 7.14: Gender distribution of respondents

Gender	Frequency	Percent	Cumulative percent
Female	285	53.1%	53.1%
Male	252	46.9%	100.0%

Table 7.15: Distribution of respondents' level of education

Level of education	Frequency	Percent	Cumulative percent
No degree or up to high school	216	40.2%	40.2%
Bachelor's degree or equivalent	255	47.5%	87.7%
Masters degree and above	66	12.3%	100.0%

A similar distribution is observed in the final study when comparing the number of Facebook friends with that reported in the pilot study. Notably, 22.2% of the respondents reported having more than 400 Facebook friends. Unlike the pilot study, the Facebook friends distribution exhibits a plateau between the category labelled 11-50, and the category labelled 201-250 (see Table 7.16).

Most of the respondents (68.7%) reported spending up to an hour a day on Facebook, with 9.1% spending more than 3 hours on Facebook daily (see Table 7.17). When it comes

Table 7.16: Distribution of number of Facebook friends

No. of friends	Frequency	Percent	Cumulative percent
10 or less	18	3.4%	3.4%
11-50	57	10.6%	14.0%
51-100	73	13.6%	27.6%
101-150	69	12.8%	40.4%
151-200	72	13.4%	53.8%
201-250	58	10.8%	64.6%
251-300	33	6.1%	70.8%
301-400	38	7.1%	77.8%
more than 400	119	22.2%	100.0%

Table 7.17: Distribution of time spent on Facebook

Minutes on Facebook	Frequency	Percent	Cumulative percent
less than 10 minutes	77	14.3%	13.3%
10-30 minutes	161	30.0%	44.3%
31-60 minutes	131	24.4%	68.7%
1-2 hours	83	15.5%	84.2%
2-3 hours	36	6.7%	90.9%
more than 3 hours	49	9.1%	100.0%

to the number of Facebook Apps used, 12.7% of respondents reported using more than nine Apps, with 4.5% being unaware as to how many Facebook Apps they are using (as per Table 7.18).

Table 7.18: Distribution of number of Facebook Apps used

No. of Facebook Apps	Frequency	Percent	Cumulative percent
1-2	229	42.6%	42.6%
3-4	130	24.2%	66.9%
5-6	69	12.8%	79.7%
7-8	17	3.2%	82.9%
more than 9	68	12.7%	95.5%
unknown	24	4.5%	100.0%

Because the scale corresponding to the construct *Facebook and PC experience* was excluded from the multivariate analysis, some of these results are reported here as part of the univariate analysis. When asked about the continued use of Facebook Apps, 42.6% of the respondents reported that they are likely to use Facebook Apps, with 6.5% reporting that it is extremely unlikely that they will continue using Facebook Apps. When reporting their confidence in using Facebook Apps, most respondents (67.6%) agreed that they are confident users of Facebook Apps. It follows that most respondents (75.6%) also reported that they are confident understanding terms/words related to Facebook Apps, in addition to working on a personal computer.

7.2.2.2 Research model constructs

The second part of the descriptive analysis consisted of an investigation of the research model's constructs. Table 7.19 presents the descriptive statistics of these constructs, with the various figures illustrating the histogram of each construct. Note that at this point the construct *Facebook usage* was also excluded since:

- It is not a core component of this study (i.e., it does not feature in any of the propositions or research questions), and
- Several of its items were found to exhibit Variance Inflation Factor (VIF) values in excess of 5.0 - thus reducing its validity.

Table 7.19: Descriptive statistics of the constructs used in the multivariate analysis

Constructs	**Mean**	**SD**
Neuroticism	3.49	1.03
Agreeableness	2.06	0.73
Extraversion	3.01	1.00
Conscientiousness	1.87	0.74
Openness to Experience	2.25	0.74
Attitude towards privacy	1.94	0.61
Social norms	3.16	1.00
Information security awareness	1.61	0.64

These histograms provide a visual impression of their respective distributions. A distribution that is right-skewed indicates that the majority of respondents obtained a lower score with only a few higher scores. The converse is applicable for a left-skewed distribution.

For example, the distribution of the scale associated with the construct *Attitude towards privacy* is skewed towards the right. From Table 7.20, it is clear that 38.9% of respondents either strongly agreed or agreed when answering the item, *It is risky to use Facebook Apps* - 27.0% were undecided in this regard. In terms of Facebook having access to users' personal information, 68.5% of respondents either strongly agreed or agreed that this is important. Furthering this, 74.5% of respondents either strongly agreed or agreed that it is good for Facebook Apps to have access to their personal information.

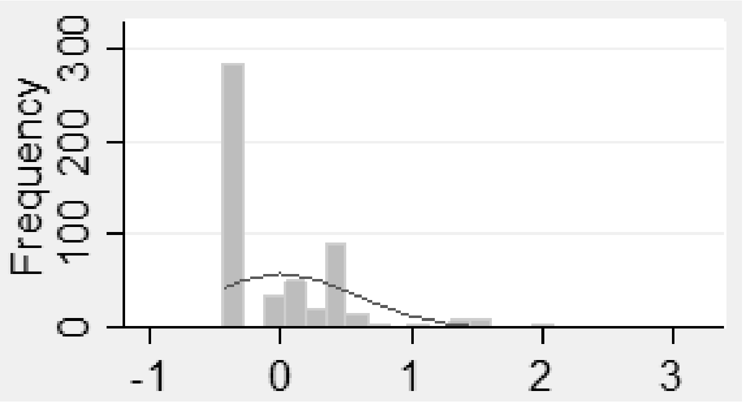


Figure 7.1: Distribution of *Attitude towards privacy*

Unlike Table 7.20, the descriptive statistics for the construct *Information security awareness* is presented in three tables. This stems from the use of three different response anchors.

Table 7.20: Univariate results of construct *Attitude towards privacy*

Item	**Strongly agree**	**Agree**	**Neither agree nor disagree**	**Disagree**	**Strongly disagree**
It is risky to use Facebook Apps.	9.1%	29.8%	27.0%	28.3%	5.8%
Using the privacy settings on my Facebook account is unnecessary.	53.1%	34.6%	6.5%	4.3%	1.5%
Using the privacy settings on my Facebook account is important.	63.1%	30.7%	3.2%	1.9%	1.1%
Using the privacy settings on my Facebook account is good.	61.8%	33.0%	4.1%	0.6%	0.6%
It is important that Facebook Apps have access to my personal information.	30.7%	37.8%	19.6%	7.1%	4.8%
It is good that Facebook Apps have access to my personal information.	37.6%	36.9%	16.4%	6.1%	3.0%
It is unnecessary for Facebook Apps to have access to my personal information.	44.7%	33.0%	12.8%	7.3%	2.0%

Table 7.21: Distribution of items relating to safety of personal information

Item	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
I must periodically review the privacy settings on my Facebook account.	38.7%	44.1%	7.1%	7.3%	2.8%
It is very important to me that I am aware and knowledgeable about how my personal information will be used.	53.4%	38.2%	5.4%	2.2%	0.7%
Companies seeking personal information online should disclose the way the data are collected, processed and used.	74.9%	19.2%	4.1%	1.5%	0.4%
I follow the news and developments about the privacy issues and privacy violations related to social media.	28.5%	46.0%	13.4%	9.9%	2.2%
I am aware of the privacy issues related to the use of Facebook Apps.	34.5%	47.1%	12.1%	4.5%	1.9%
I believe I have control over who can get access to my personal information collected by Facebook Apps.	13.4%	27.4%	20.7%	29.2%	9.3%

As presented in Table 7.21, 82.8% of respondents expressed overall agreement that it is a good idea to review their privacy settings periodically. Additionally, 91.6% of the respondents also agreed that awareness of secondary use of personal information is important. This aligns with the finding that, 94.1% of respondents agreed that companies should explain how they use personal information. Although most (91.6%) of the respondents agreed that it is important to be aware as to how their personal information is used, fewer respondents (74.5%) stayed abreast of social media privacy issues. Furthermore, most of the respondents agreed that they are indeed aware of the privacy-related issues when using Facebook Apps. When asked about whether respondents feel that they control their personal information, 20.7% were unable to either disagree or agree.

When measuring information privacy concerns (see Table 7.22), more than half of the respondents reported being moderately or extremely concerned with the level of access friends' Facebook Apps have to their personal information. In the event that a friend's Facebook App collected personal information of the respondent, higher levels of concern were expressed as opposed to the respondent's apps collecting information about their friends. Additionally, 65.2% reported being either moderately or extremely concerned about the Facebook App used to collect the personal information which was ultimately abused by Cambridge Analytica (Coldewey, 2018).

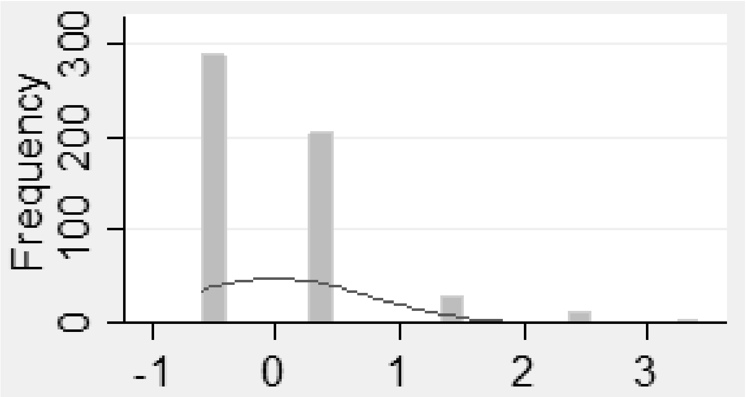


Figure 7.2: Distribution of *Information security awareness*

The distribution of the personality constructs is of particular importance with *Extraversion* normally distributed as opposed to the other constructs. For example, *Openness to Experience*, *Conscientiousness* and *Agreeableness* are all skewed towards the right. Conversely, *Neuroticism* is skewed towards the left. The personality-based histograms are illustrated in Figures 7.4 through 7.8.

Table 7.22: Distribution of items relating to the privacy of their personal information

Item	**Not at all concerned**	**Slightly concerned**	**Somewhat concerned**	**Moderately concerned**	**Extremely concerned**
The default privacy settings on Facebook allow my friend's Apps to collect my personal information.	6.3%	21.4%	19.0%	25.0%	28.3%
Facebook does not notify me in advance of the possibility that one of my friend's Apps is going to collect personal information about me.	5.6%	14.0%	19.2%	24.2%	37.1%
Facebook does not notify me in advance of the possibility that one of my Apps is going to collect personal information about my friends.	5.2%	11.5%	21.2%	28.1%	33.9%
Facebook does not ask for my approval in advance of the possibility that one of my friend's Apps is going to collect personal information about me.	4.7%	13.0%	17.5%	23.8%	41.0%
A Facebook App (thisismydigitallife) was identified as the source of personal information that was abused by Cambridge Analytica.	7.4%	8.6%	18.8%	21.4%	43.8%

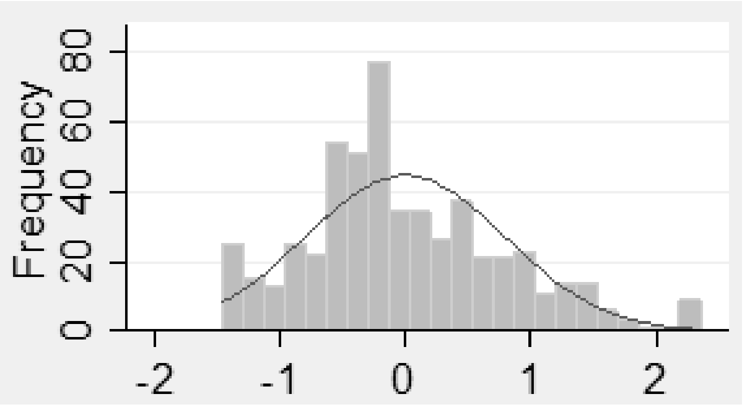


Figure 7.3: Distribution of *Social norms*

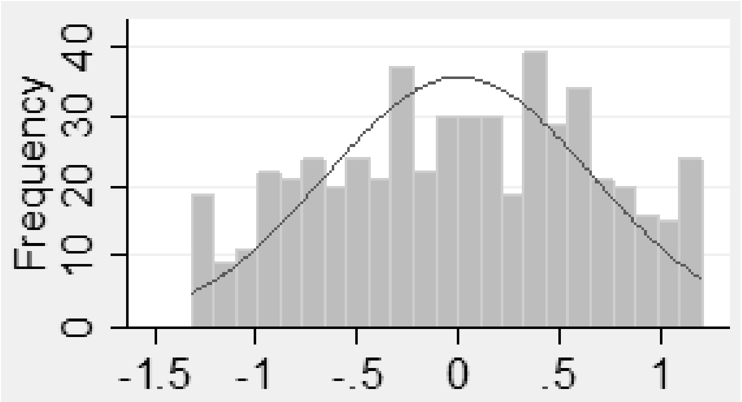


Figure 7.4: Distribution of *Extraversion*

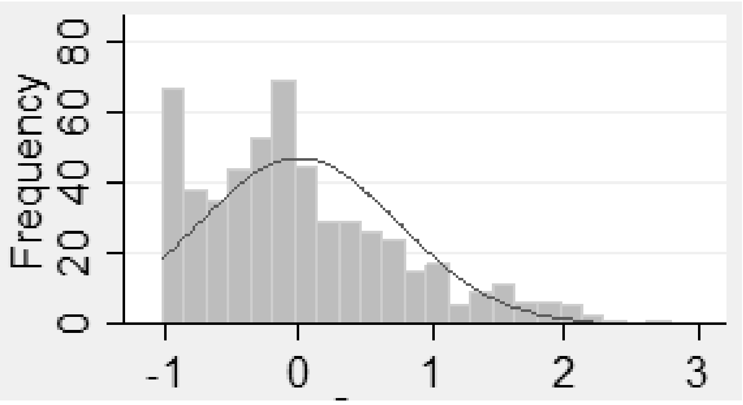


Figure 7.5: Distribution of *Openness to Experience*

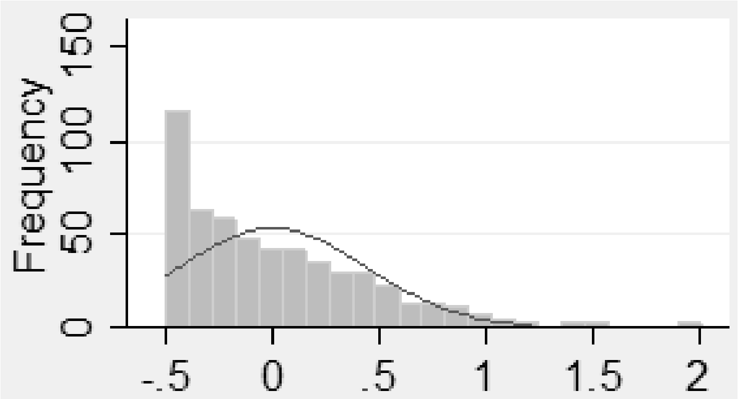


Figure 7.6: Distribution of *Conscientiousness*

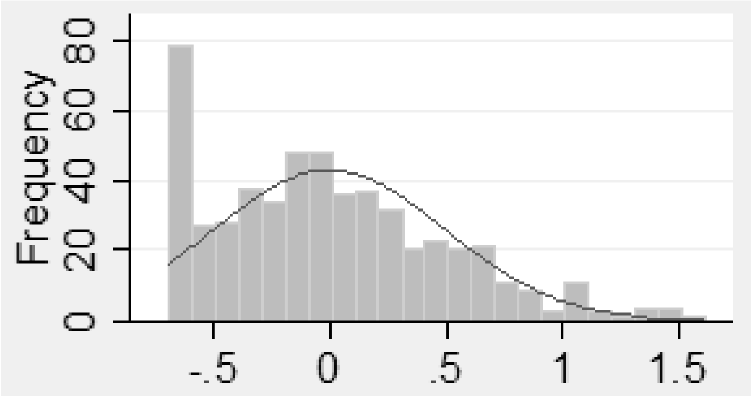


Figure 7.7: Distribution of *Agreeableness*

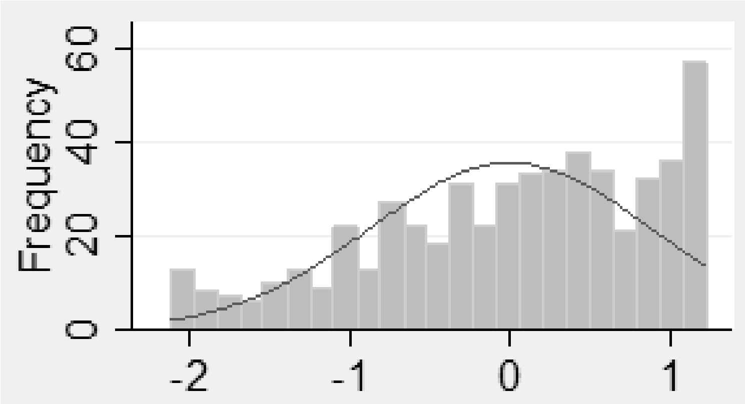


Figure 7.8: Distribution of *Neuroticism*

As stated, the aforementioned histograms and descriptive statistics are used to supplement the discussions related to this study's research questions.

7.2.3 Assessing the measurement model

After cleaning the dataset an Exploratory Factor Analysis (EFA) was conducted (Kelloway, 1995) as part of the first step towards assessing factorial validity and reliability. This entailed establishing the validity of the items distributed across eight constructs presented in the measurement model. Firstly, convergent validity was assessed by examining the outer loadings of the questionnaire items against their relevant constructs. More specifically, every item's outer loading had to exceed the threshold of 0.50 and exhibit significant t-statistic values (Hair et al., 2013; James et al., 2017). To satisfy these conditions, several items had to be dropped as outlined in Appendix A.

Secondly, discriminant validity was assessed by comparing the square root of each Average Variance Extracted (AVE) value with all the correlations associated with that specific construct. These are presented as the values on the diagonal of the measurement model statistics (Table 7.23). To satisfy the condition of discriminant validity, each of these values should be higher than any of the other correlations that involve that specific construct (Fornell & Larcker, 1981; James et al., 2017). All the values satisfied the latter condition; thus establishing discriminant validity.

The process of establishing factorial validity also included checking for multicollinearity. All items displayed a Variance Inflation Factor (VIF) below 5, except two items from the *Facebook usage* construct. Since this construct does not form a core component of this study and is earmarked for future research, it was excluded from the multivariate analysis, as mentioned earlier in this chapter. In turn, the removal of the *Facebook usage* construct enabled the questionnaire to eliminate multicollinearity as a problem going forward (see Appendix C for all the VIF values).

To assess the overall reliability of the constructs, both Cronbach's alpha (CA) and Composite Reliability (CR) values were calculated. The CA and CR values attest to how internally consistent a construct is with values in excess of 0.70 satisfying this condition (Cronbach, 1951). All of the constructs exhibited CA and CR values above 0.70 and were thus deemed reliable (see Table 7.23 for each construct's CA and CR value).

Table 7.23: Measurement model statistics, reliability and AVE values

Construct	CR	CA	AVE	1	2	3	4	5	6	7	8
Neuroticism	0.913	0.911	0.571	**0.756**							
Agreeableness	0.845	0.840	0.380	-0.468	**0.617**						
Extraversion	0.893	0.893	0.515	-0.357	0.229	**0.718**					
Conscientiousness	0.888	0.878	0.470	-0.510	0.474	0.223	**0.686**				
Openness to Experience	0.866	0.857	0.403	-0.209	0.215	0.332	0.239	**0.635**			
Attitude towards privacy	0.737	0.762	0.321	-0.025	0.132	-0.047	0.168	0.096	**0.567**		
Social norms	0.888	0.891	0.537	-0.094	0.141	0.142	0.089	0.019	-0.541	**0.733**	
Information security awareness	0.857	0.856	0.375	-0.042	0.032	0.015	0.015	0.286	0.530	-0.133	**0.613**

7.2.4 Assessing the structural model

The multivariate analysis aimed to ascertain the extent of the influence of the constructs *Social norms*, *Attitude towards privacy* and *Information security awareness* on the dependent variable *Intention to use Facebook Apps*. This was calculated using Partial Least Squares (PLS) path modelling, culminating in the development of this study's structural model (see Figure 7.9).

SmartPLS 3 was used to evaluate the structural model. This involved calculating the path coefficients, predictive power (R^2), effect sizes (f^2), and predictive relevance (Stone-Geisser's Q^2) (Geisser & Eddy, 1979; Stone, 1974). These values are all presented in Table 7.24 (end of Section 7.2.4). The in-sample predictive power of the model was found to be substantial (0.857) indicating that together, the model's independent constructs (variables) account for 85.7% of the variance in the dependent construct (variable) (*Intention to use Facebook Apps*). The out-of-sample predictive power of the model was calculated at 0.350 (Q^2), with values in excess of zero indicating that the structural model possesses predictive relevance outside the data used to estimate the structural model (Hair et al., 2017). These results provide evidence to suggest that the model is structurally sound.

7.2.4.1 Evaluation of propositions

The aim of this study's propositions was to establish the extent to which the listed constructs influence a Facebook user's intention to make use of Facebook Apps:

- Attitude towards privacy,
- Social norms,
- Information security awareness, and
- The five personality constructs (corresponding to the Big Five personality traits).

To evaluate the research model constructs, the structural model incorporated path analysis, which not only indicated the strength (weight) of the relationships between the constructs (latent variables) but also whether these are statistically significant. See Table 7.24 for all the paths' estimates, effect sizes, t-statistics, and overall statistical significance. From a propositional perspective, these results are indicative of the following:

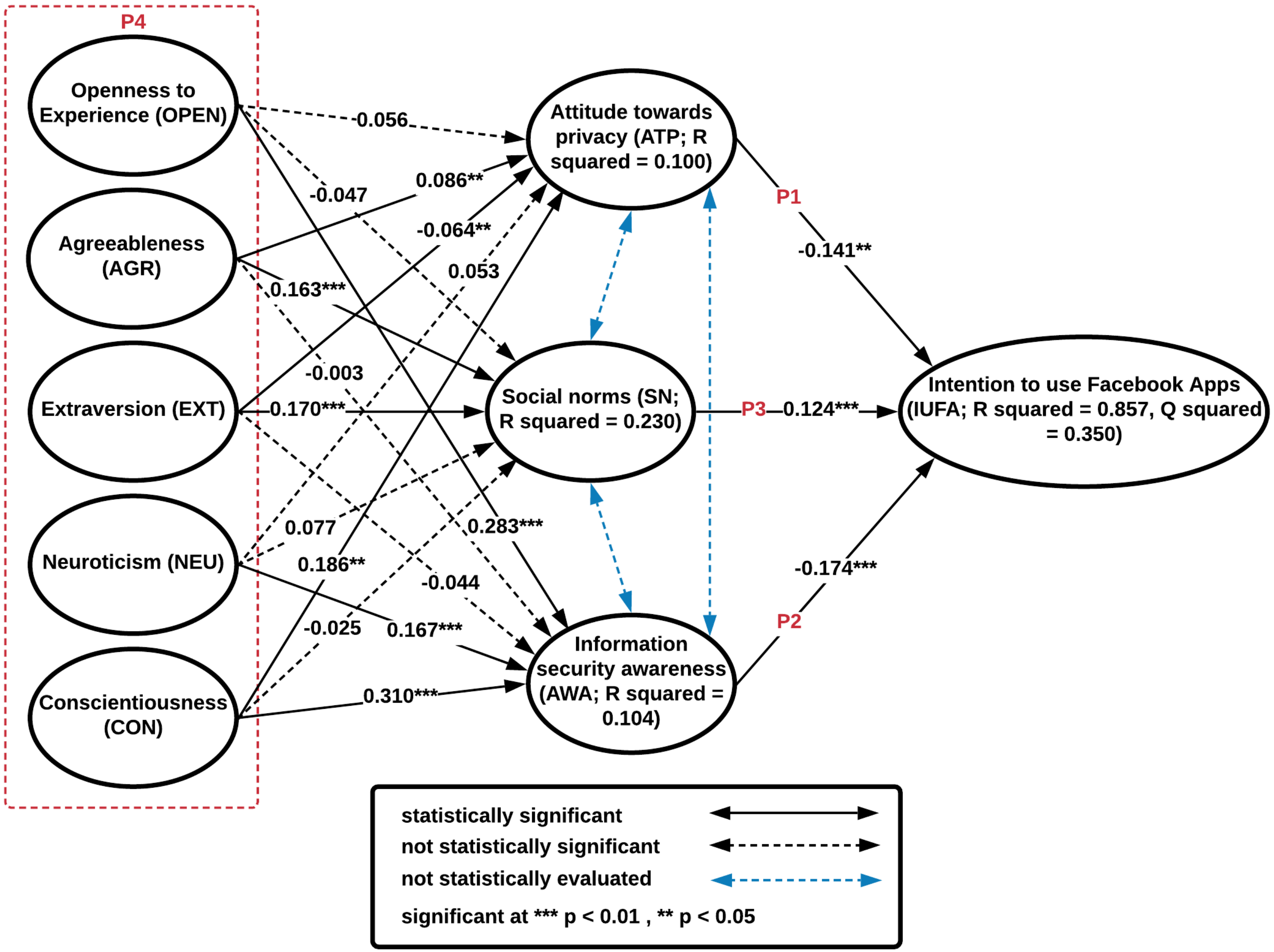

P4
Openness to Experience (OPEN)
Agreeableness (AGR)
Extraversion (EXT)
Neuroticism (NEU)
Conscientiousness (CON)
-0.056
-0.047
0.086**
-0.064**
0.053
0.163***
-0.003
0.170***
0.077
0.283***
0.186**
-0.044
-0.025
0.167***
0.310***
Attitude towards privacy (ATP; R squared = 0.100)
Social norms (SN; R squared = 0.230)
Information security awareness (AWA; R squared = 0.104)
P1
-0.141**
P3
-0.124***
P2
-0.174***
Intention to use Facebook Apps (IUFA; R squared = 0.857, Q squared = 0.350)
statistically significant
not statistically significant
not statistically evaluated
significant at *** p < 0.01 , ** p < 0.05

Figure 7.9: Personality-based Facebook App surveillance model

- The first proposition (P1) states that a Facebook user's attitude towards privacy will influence their intention to use Facebook Apps. This corresponds to the path between *Attitude towards privacy* and *Intention to use Facebook Apps* - a statistically significant (p<0.05) and negative influence. This result provided support for the first proposition and exhibits a small effect size Cohen (1988).

- The second proposition (P2) states that an individual's information security awareness will influence their intention to use Facebook Apps. This is illustrated as the path between *Information security awareness* and *Intention to use Facebook Apps* - a statistically significant (p<0.01) and negative influence. This result provided support for the second proposition and exhibits a medium effect size (Cohen, 1988).

- The third proposition (P3) states that social norms will influence an individual's intention to use Facebook Apps. This corresponds to the path between *Social norms* and *Intention to use Facebook Apps* - a statistically significant (p<0.01) and positive influence. As such, this result provided support for the third proposition and exhibits a medium effect size (Cohen, 1988).

- The fourth proposition (P4) states that an individual's personality will influence their intention to use Facebook Apps. Unlike the aforementioned propositions, this proposition is evaluated by 15 paths (originating inside the red dotted rectangle in Figure 7.9). Results indicate that of the 15 paths, seven are not statistically significant (see Table 7.24). As such, eight paths were found to be statistically significant, thus providing partial support for this proposition. Of all the statistically significant relationships *Openness to Experience* exhibited the largest effect size on *Information security awareness* (large effect) and thus contributed the most to the predictive power (R^2) of *Information security awareness* (Hair et al., 2017). On the other hand *Conscientiousness* exhibited the largest effect size on *Attitude towards privacy* (medium effect) with *Extraversion* exhibiting the largest effect size on *Social norms* (medium effect).

The results of the statistically significant paths, related to the personality-based constructs are as follows:

- The path between *Extraversion* and *Attitude towards privacy* was found to be statistically significant (p<0.05) and negative.

- The path between *Extraversion* and *Social norms* was found to be statistically significant (p<0.01) and positive.
- The path between *Agreeableness* and *Attitude towards privacy* was found to be statistically significant (p<0.05) and positive.
- The path between *Agreeableness* and *Social norms* was found to be statistically significant (p<0.01) and positive.
- The path between *Conscientiousness* and *Attitude towards privacy* was found to be statistically significant (p<0.05) and positive.
- The path between *Conscientiousness* and *Information security awareness* was found to be statistically significant (p<0.01) and positive.
- The path between *Neuroticism* and *Information security awareness* was found to be statistically significant (p<0.01) and positive.
- The path between *Openness to Experience* and *Information security awareness* was found to be statistically significant (p<0.01) and positive.

7.3 Summary

The objective of this chapter was to provide a detailed result-centric overview of the pilot and the final study. The results of the pilot study were presented with a specific focus on validity and reliability, data collection, as well as the resultant univariate analysis of the collected data. Of particular importance was the section that detailed the changes that were made after conducting the pilot study. This was followed by the results of the final study, including aspects relating to the demographics and data collection. However, unlike the pilot study, which only analysed the data in a univariate manner, the final study also comprised a multivariate component. Results about factorial validity and reliability were presented, followed by the measurement model and the structural model. The chapter concluded with an outline of the structural model's paths estimates and to what extent these provide support

Table 7.24: Path estimates of structural model

Path	β	**f ^{2}**	**t-statistic**	**Supported**
EXT - > ATP	-0.064**	0.014	-1.97	Yes
EXT - > AWA	-0.044	0.002	-1.29^{ns}	No
EXT - > SN	0.170***	0.312	4.11	Yes
AGR - > ATP	0.086***	0.113	2.09	Yes
AGR - > AWA	-0.003	0.008	-0.08^{ns}	No
AGR - > SN	0.163***	0.216	3.16	Yes
CON - > ATP	0.186**	0.153	2.88	Yes
CON - > AWA	0.310***	0.353	4.45	Yes
CON - > SN	-0.025	0.002	-0.31^{ns}	No
NEU - > ATP	0.053	0.035	1.39^{ns}	No
NEU - > AWA	0.167***	0.216	4.04	Yes
NEU - > SN	0.077	0.013	1.62^{ns}	No
OPEN - > ATP	0.056	0.098	1.39^{ns}	No
OPEN - > AWA	0.283***	0.732	6.3	Yes
OPEN - > SN	-0.047	0.003	-0.93^{ns}	No
ATP - > IUFA	-0.141**	0.115	-2.10	Yes
AWA - > IUFA	-0.174***	0.258	-3.45	Yes
SN - > IUFA	0.124***	0.270	4.87	Yes

*** = significant at $p<0.01$
** = significant at $p<0.05$
ns = not significant
R^2 of structural model = 0.857
Q^2 of structural model = 0.350

for this study's propositions. In the following chapter, a detailed discussion will be presented with a particular focus on how these results address not only the research questions but also the problem statement.

Chapter 8

DISCUSSION

> "To explain all nature is too difficult a task for any one man or even for any one age. Tis much better to do a little with certainty and leave the rest for others that come after you."
>
> — Isaac Newton

This chapter provides a detailed discussion of this study's results. It provides additional insight as to how the results and extant literature apply to the thesis problem, namely information security awareness within a surveillance context - specifically Facebook Apps. Importantly, the context of this study is theorised throughout, by making specific reference as to how the attitude, social norms, and awareness contribute to the results illustrated by the structural model. This is especially pertinent in those cases where the influence of specific personality traits was not statistically significant.

8.1 Introduction

As stated in Chapter 3, it is in the best interest of social media corporates not only to entice new users, but also to engage current users in a manner that amplifies their desire for information. Such forms of amplification takes place by appealing to an individual's need to develop on a psychosocial level. As such, everyday communicative acts, such as sharing thoughts and ideas with friends and family, have been digitised and made readily available through the use of social media platforms. For example, it is relatively easy to start using

Facebook since it is pre-installed on most mobile phones. Given that 72% of US citizens reported using social media services on a variety of devices (Pew Research Center, 2019b), it increases the likelihood that users will either start or continue making use of these services.

More users leads to more content creation and consumption, which leads to more capital growth on the part of the social media platform due to targeted advertising and secondary use of personal information. The users of these social media platforms, however, are more focused on other matters, such as sharing and building relationships with other Facebook users, which this study argues is influenced by factors such as attitude, social norms, and information security awareness.

As part of the latter argument, this study collected data from United States (US) citizens to ascertain to what extent these factors influence the intended use of Facebook Apps. Measuring the intended use of Facebook Apps within a surveillance context is not new; however, to address the psychosocial aspect of social media use, the study also evaluated the influence of personality traits - specifically the Big Five.

8.2 The significance of attitude

The results are indicative that the respondents were influenced by their *Attitude towards privacy*. This construct (adapted from the Theory of Planned Behaviour) comprised items that evaluated respondent attitudes towards the privacy of their personal information — captured by asking questions relating directly to Facebook Apps or Facebook privacy settings. In this regard, a statistically significant (-0.141** at p<0.05) and a negative relationship was observed between the variables *Attitude towards privacy* and *Intention to use Facebook Apps*. Given that the attitudinal items used in the multivariate analysis (items 65, 66 and 67) all questioned respondents about the use of their Facebook privacy settings, it is clear that respondents' attitudes towards the use of privacy settings make them less likely to use Facebook Apps. As such, even though respondents placed emphasis on the use of these settings, they are still inclined not to use these Apps. This may indicate that respondents are somewhat apprehensive when deciding whether or not they should use Facebook Apps - even if they use privacy settings. It is plausible that such apprehension is not only rooted in the usefulness of Facebook privacy settings, but also to what extent they trust (see Section 5.2.3) and are alienated by Facebook (Ortiz et al., 2018); specifically with regard to the safekeeping of their personal information.

8.2.1 Attitude towards information privacy

The univariate results of this study indicate that the respondents deemed the use of Facebook privacy settings to be both important and good (see Table 7.20). Nevertheless, a negative relationship between *Attitude towards privacy* and *Intention to use of Facebook Apps* is observed. It thus seems that respondents value or at least report that they value the privacy of their personal information, and are likely to safeguard it, using privacy settings. Accordingly, the negative influence on intended use further indicates that respondents may feel that Facebook Apps can circumvent these settings and thus gather personal information regardless of privacy settings. This is not surprising, given the number of public incidents that not only attest to the general misuse of Facebook-based information, but also personal information gathered through the use of Facebook Apps. One example being the App, *thisismydigitallife*, developed by Alexandr Kogan; a prominent figure within the Cambridge Analytica incident referred to in Chapter 3.

Respondents may also treat the effectiveness of privacy settings with suspicion because of the large number of device manufacturers that have been granted privileged access to the platform (see Section 3.5). It is thus likely that an awareness of such matters may dissuade respondents from using Facebook Apps; especially since United States citizens are subject to surveillance under the Patriot Act (via the PRISM programme) (Snowden, 2016). The fact that social media corporates have been implicated in funnelling data to intelligence agencies under the PRISM programme further contributes to suspicion (see Section 3.4) (Snowden, 2016).

Psychological aspects such as a user's personality also influence suspicion (Hilton et al., 1993). Given that the surveillance mentioned earlier is performed on personal information provided or shared by a user, this study classifies these activities as self-disclosure. It thus follows that the sharing of personal information is also subject to a user's attitude towards self-disclosure (Kezer et al., 2016). In this regard, there is some overlap with Facebook Apps. For example, most Facebook Apps (also third-party-developed) will notify users as to what information is required to use the App - albeit obfuscated in some instances. Thus, such self-disclosure is performed by choice, based on the amount of risk perceived and the proclivity of the individual's personality traits to accept said risk.

Here, theory suggests that a heightened perception of risk will lead to a positive attitude towards secure behaviour (see Section 5.2.1). This study's univariate results confirm this, with most respondents viewing Facebook Apps as risky. The multivariate results follow suite, indicating the existence of a negative relationship between attitude (specifically the privacy settings) and intended use of Facebook Apps. The negative influence on *Intention to use Facebook Apps* finds some parallel with other studies reviewed. For example, in Section 5.4.2, it is stated that the study conducted by Karwatzki et al. (2017) found that individuals who hold information privacy in high regard are less likely to disclose information. Thus, a positive attitude towards privacy (privacy settings in this context) led to a reduction in the intention to disclose.

Their perception of risk may also influence Facebook users' appraisal of how easy it is to cope with the use of privacy settings. If these settings are perceived to be complicated and challenging to use, users may perceive themselves less effective at using them appropriately; thus, increasing the perceived risk of disclosing personal information to unwanted third-parties. It is thus plausible that respondents may view the use of Facebook Apps as yet another set of complex interfaces and settings they have to use. Thus, further dissuading overall intent to use Facebook Apps.

As the literature review found, users are inclined to comply with security policies (Section 6.2.1) given their positive attitude, and likewise, some Facebook users are likely to avoid Facebook Apps due to their attitude towards privacy. This is an interesting finding considering that the univariate analysis indicated that respondents mostly viewed the privacy settings as good, important, and not unnecessary. Such views may be indicative of two aspects. Firstly, respondents may feel a sense of distrust towards Facebook. The use of privacy settings and thus secure behaviour is viewed as important, but not necessarily sufficient to protect personal information, given recent experience in this regard. For example, even though users make use of privacy settings and passwords, their information is still being disclosed and misused through an ever-increasing amount of information breaches (see Section 3.4.1).

Secondly, respondents behave differently to what is reported, due to differences in how they perceive privacy and risk. Based not only on experience (see Section 5.2.3), but also on their personality. For example, this study has found that the respondents reported valuing their personal information by expressing positive views of Facebook privacy settings. As per the Privacy Paradox (Kokolakis, 2017), these participants subsequently reported that they are less likely to use Facebook Apps - as confirmed by the multivariate results. Recent surveys in the United States suggest otherwise, with a more diverse (i.e., different age groups) set of users making use of Facebook and associated Apps than ever before (Pew Research Center, 2019a). Thus, contrary to the research of Karwatzki et al. (2017) and Vladlena et al. (2015) respondent concerns over the privacy of their personal information (also reported in this study's results) does not dissuade users from the actual use of Facebook Apps. Thus, unlike the literature reviewed (in section 5.2), results indicate that Facebook's privacy mechanisms (the privacy settings) fail to ameliorate privacy concerns (see Table 7.22), even though most respondents viewed the use of such settings as something important.

In reality, actual use persists, which may indicate that in theory, respondents know they ought to be concerned about their personal information, but still behave differently. Some respondents may also not be aware and knowledgeable enough about the risks and thus continue using Facebook Apps. Here, privacy settings may seem like a good idea, although they have no idea how to use them or if they do, it's possibly too complex for them to use such settings.

It is thus plausible that other factors influence the perception mentioned above. These include their views on risk, information privacy, and Facebook privacy settings, as well as respondents' attitude towards these; one such group of factors being individual differences. As such, this study argues that it is only through a discussion of individual differences (i.e., personality traits) and their resultant influence on a user's attitude towards privacy, that one can adequately explain the negative relationship illustrated in the structural model (see Figure 7.9).

8.3 Information security awareness and privacy

As illustrated in the structural model (Figure 7.9) a negative and statistically significant (-0.174*** at p<0.01) relationship exists between *Information security awareness* and *Intention to use Facebook Apps*. As such, as awareness increases so does respondents' intention to use Facebook Apps decrease, based on their concerns and awareness regarding the privacy of their personal information.

In Section 5.4.1, it was argued that an increase in awareness leads to the acquisition of more knowledge, as illustrated through the process of subsidiation. For example, an increase in awareness of government surveillance through the process of subsidiation leads to a change in attitude towards such forms of surveillance. Awareness could also be influenced by *Social norms* and *Attitude towards privacy* as prescribed by the TPB (though not statistically evaluated in this study).

Ortiz et al. (2018) also found social media users to be more likely to value the privacy of their personal information as awareness levels increase. Unlike this study, the latter study separated information privacy concerns from information security awareness, yet still managed a similar direct influence from information security awareness to the dependent variable (privacy risk belief). Interestingly, Ortiz et al. (2018) also discusses the concept of alienation, whereby social media users are somehow aware of the information privacy issues, but feel that they cannot ameliorate them. The more these users' awareness increases, the more alienated and problematic social media use becomes (i.e., it paradoxically increases), leading to the development of a negative attitude towards information privacy on these platforms. This finding of Ortiz et al. (2018) contradicts this study's results concerning information security awareness because of the negative relationship between *Information security awareness* and *Intention to use these Facebook Apps*.

Flores & Ekstedt (2016) also separated information security awareness, making use of similar TPB-based constructs. However, unlike Ortiz et al. (2018) awareness is modelled as an antecedent of self-efficacy (argued as an equivalent of Perceived Behavioural Control in this study). Flores & Ekstedt (2016) also found self-efficacy to have a weak relationship on the dependent variable in their study (intention to resist social engineering). Since self-efficacy is argued (Section 5.4) to be part of the construct *Information security awareness*, this shares some similarity with this study's results (i.e., some of the path coefficients are lower than others).

By way of examining the dependent variables of the study conducted by Flores & Ekstedt (2016), and this study's dependent variable, it is possible to observe some common ground. For example, Facebook users and employees may share the same level of alienation. In other words these users may believe it futile to try and prevent either having their personal information misused, or falling victim to social engineering attacks. As such, no level of self-efficacy (part of awareness in this context) is ever really enough to circumvent these. It is true that awareness is negatively related with *Intention to use Facebook Apps*; however, as mentioned earlier, this is not reflected in the figures of actual use. Again, users may believe that they know they should be concerned, given their awareness of these surveillance matters, but also know that there is not much they can change in this regard (i.e., they feel that they are not in control).

Whereas the lack of control influences awareness as described above, the presence thereof has been proven to have the opposite effect. Given that this study's focus is on Facebook Apps (and the settings Facebook provides), it is somewhat understandable that users do not feel that they have complete control of their personal information (i.e., it is stored and secured by Facebook). It thus makes sense that Hanus & Wu (2016) found conflicting results. In their study, they focused on information security awareness of desktop computers, where users are generally in control. Interestingly, their model results (based on Protection Motivation Theory) also state that self-efficacy explains approximately 23.7% of the variance, but exhibits a stronger influence on the dependent variable in their context. These results indicate that efficacy (either self or response based) is essential when modelling awareness - primarily since the other relationships in their study were not found to be statistically significant.

Within the realm of Facebook Apps users have little control over how their personal information is used. This lesser amount of control not only ties into the results of the aforementioned studies, but also provides additional evidence as to the relatively weak strength of the resultant relationships between *Information security awareness* and *Intention to use Facebook Apps*. For example, if this study were to have included items that measured efficacy and control, the resultant relationship's path coefficient might have been different (i.e., users are more aware of how little control they have); in turn, decreasing their intention to use Facebook Apps.

From the univariate analysis, it is clear that most respondents agree (91.6%) that the use of their personal information is worth knowing about. Because this item (second row in Table 7.21) is combined with the rest of the items that evaluate awareness, it is not possible to isolate its multivariate effect. It does, however, enrich the theoretical discussion about the blue dotted relationship between *Information security awareness* and *Attitude towards privacy*. For example, in the discussion about the significance of attitude, it was argued that the relationship is relatively weak and that if it was statistically evaluated may have yielded interesting additional results - specifically in relation to the construct *Information security awareness*. If evaluated, the latter relationship would have likely influenced the relationship between *Attitude towards privacy* and *Intention to use Facebook Apps*. Mainly because the fact that additional awareness as to secondary use of personal information would likely cause an individual to value privacy settings more. Evidence of this is reported in a study about information disclosure on social media sites in general, where the authors used an experimental approach to make users more aware of the risks to their personal information (Padyab et al., 2019). For example, once users were made aware of the use of their personal information post-disclosure, their attitude changed from affective to cognitive. Such a cognitive approach to privacy lends itself to the use of mechanisms such as privacy settings, which in the context of this research, could account for both the theoretical influence indicated as per the dotted blue line and the relatively weak relationship between *Attitude towards privacy* and *Intention to use Facebook Apps*. In other words, the more aware a user is, the more likely they are to use privacy settings.

8.4 Social norms

As defined in Section 5.3, this study considers both subjective and descriptive norms to form part of social norms. Accordingly, the questionnaire includes items that evaluate both the perception of what significant others and peers think one should do (subjective - items 75 to 77) as well as that which significant others and peers are perceived to do (descriptive - items 71 to 74).

As per the structural model (Figure 7.9), there is a positive and statistically significant relationship between *Social norms* and *Intention to use Facebook Apps* (0.124*** at p<0.01). Because social norms contain both subjective and descriptive norms, it plays an important part within the context of this study. This stems from the fact that it influences both information security awareness and attitude, and because it encapsulates that which is social media. After all, social media is a platform that thrives not only on the surveillance conducted by the platform, but also the surveillance amongst members of the platform (i.e., looking at what others are posting and liking, for example).

As with the other constructs (i.e., attitude and awareness), this relationship is also relatively weak. It is thus possible that the same bi-directional relationships (indicated as blue dotted lines in Figure 7.9) would have further influenced the magnitude of this value. For example, if a family member expresses his or her concern over the safety of their personal information, the theory suggests (as per Section 5.3) the other family members are likely to be influenced as well. Given the overall negative relationship between *Information security awareness* and *Intention to use Facebook Apps* it is likely to have further influenced the relationship. Additionally, this increased awareness through the interaction with other family members would have also further influenced the path coefficient of the relationship between *Social norms* and *Intention to use Facebook Apps*. For example, one family member's concern could ultimately influence the rest of the family, resulting in a lower intention to use Facebook Apps. It is, however, interesting that this relationship is positive, unlike that of *Attitude towards privacy* and *Information security awareness*. This means that based on the influence of significant others, respondents displayed an intention to use Facebook Apps. This may suggest that *Social norms* mostly accounts for the positive influence on *Intended use of Facebook Apps*. In turn, this indicates that the influence of significant others plays a pivotal part in the intended use of Facebook Apps. More so than only attitude or only awareness.

Similar studies confirm the significant influence of social norms on social media. For example, Zlatolas et al. (2019) found that privacy-specific social norms significantly (and positively) influence an individual's disposition for privacy. Additionally, Kamleitner & Mitchell (2019) found that social norms play a more central role when it comes to privacy protection behaviour. So much so, that it ranked as important as privacy behaviour initiated out of self or financial interest in their quest to develop a privacy-centric framework. In turn, this indicates just how important the views of one's social group or family is; especially within the context of information privacy. Some social media users also adhere to platform-based social norms simply because they fear being alienated or confronted for not doing so. For example, if an individual's entire family makes use of Facebook Messenger as a means to communicate, those family members who do not use it are more likely to feel alienated, because of their inability to join in the communication. As such, they decide to use the App even though they may not wish to do so. This shares many similarities with the concept of social norms, as discussed by Anderson et al. (2016). In the latter study, the authors argue that sharing personal information on Facebook carries a certain amount of social value. To put this in context consider the following: Theory suggests (as per Section 5.3) that the behaviour of more senior group members are likely to influence (to a greater extent) the behaviour of others in the same group. If, for example, in a familial environment older brothers play gamified Facebook Apps (also viewed as a type of App in this context) and subsequently use these leaderboards as a form of social value, it is likely to also influence the other siblings to use the App; irrespective or any privacy concerns. Hence, the significant and positive relationship between *Social norms Intention to use Facebook Apps* in this context.

8.5 The extent of personality's influence

As stated earlier, it is plausible that an additional layer of influence exists when considering self-disclosure, privacy, awareness and risk perception. Specifically, within the context of the relationship between respondents' *Attitude towards privacy* and their *Intention use of Facebook Apps*. One such form of additional influence that is tied into both the psychological appeal of Facebook Apps, self-disclosure, privacy, awareness and risk perception is an individual's personality. Whether situational, environmental or genetic, an individual's personality predisposes them to behave in specific ways, as determined by their attitude towards objects or situations (see Section 5.2). Note that the influence of personality does not override the basic need to communicate, but rather compliments it. For example, both an individual high in Extraversion and Conscientiousness exhibits a desire to communicate - albeit to different degrees depending on their attitude towards enacting a behaviour in a given situation or environment. Chapter 4 (section 4.2.1), argued that each of the Big Five personality traits possesses different characteristics which not only influence an individual's attitude, but also their approach to behaviour in general. In this instance, their proclivity to value the privacy of their personal information by securing it with Facebook privacy settings. However, using Facebook privacy settings in this manner is based on the extent to which they perceive such behaviour to be risky. At a latent level, their perception of risk may also be influenced by self-efficacy to secure their personal information. It is thus the combined influence of a respondent's personality, their views of privacy settings, their perception of risk and overall level of self-efficacy (latent), which influence their attitude towards the use of Facebook Apps.

Importantly, the influence of the factors mentioned above is primarily determined by these individuals' level of awareness and knowledge. Specifically regarding the security of their Facebook-based personal information. Not just from the perspective of the mechanisms to use (privacy settings, for example), but also why individuals should make use of these mechanisms. Both of which are the result of sentiment formation, as described in Figure 5.1. The more aware and knowledgeable a Facebook user becomes regarding the privacy of their personal information, the more positive an attitude they develop towards the use of said privacy settings. Note that the direct influence of awareness on attitude is not evaluated empirically. It is, however, argued to be a core component of attitude formation (see section 5.1.1) and possibly another reason why the relationship within the current structural model is relatively weak.

8.5.1 Openness to Experience personality trait

8.5.1.1 Attitudinal influence

In the structural model, Openness to Experience (also referred to as Openness) was found not to have a statistically significant relationship with *Attitude towards privacy*. Given that in this context attitude is primarily shaped by respondents' views on privacy settings, a negative attitude towards privacy is not wholly unexpected; mainly because open individuals are not only less likely to conform, but also likely to engage in risky behaviour (see Section 4.3). As such, although most respondents view privacy settings positively, individuals high in Openness to Experience are not likely to follow suit. As such, for respondents high in

Openness to Experience, the use of privacy settings are not viewed as a significant reason to influence their attitude towards the intention to use Facebook Apps.

From the literature reviewed in Chapter 4, it was argued that Openness to Experience significantly influences specific social media behaviour. For example, James et al. (2017) found that Openness to Experience fully moderates individuals' fear of missing out, anxiety and envy when using social networks. Additionally, Hollenbaugh & Ferris (2014) found a significant relationship between Openness to Experience and the variety of topics these users posted about on Facebook. However, none of the findings are directly related to the use of Facebook Apps - an additional argument that provides support as to why the relationship between *Openness to Experience* and *Attitude towards privacy* is not significant.

Lane & Manner (2011) provides further support for the argument. In their study, they found that Openness to Experience was not positively related to any of the functions associated with Smart Phone use. This included use cases such as listening to music or playing games. Given that the purchase of Facebook App games attributes towards a large percentage (75%) of Facebook App use (Graham, 2019), it is plausible that individuals high in Openness to Experience view the use of Facebook Apps as a leisure activity. Additionally, since most of the Facebook Apps used are categorised into leisure-oriented categories (*Just for Fun* and *Gaming*) (Lorica, 2008) it is also difficult to argue in favour of a significant relationship between *Openness to Experience* and *Intention to use Facebook Apps*, since personality theory (Chapter 4) regards open individuals to be intellectual. Individuals high in Openness to Experience are thus likely to use educational Apps, more so than those leisure-oriented. The findings of Eşkisu et al. (2017) further strengthen this argument, where a significant relationship between Openness to Experience and the use of Facebook for educational purposes is reported. These findings may imply that individuals high in Openness to Experience view Facebook Apps as a separate use case from merely using the Facebook platform itself. According to Fayn et al. (2015) this may well be the case given that their study found evidence to suggest that individuals high in Openness to Experience view interest in a subject or object as something independent of understanding these subjects and objects.

Thus, if most Facebook Apps are indeed leisure-oriented, it stands to reason that these require less or at least a different kind of understanding and cognition than communicating and building relationships on Facebook. Given that the study of Eşkisu et al. (2017) focused on the frequency of Facebook use - a likely result of exploration - their findings further support individuals high in Openness to Experience viewing Facebook Apps as a different use case. A use case where information privacy (and related settings) is not viewed as crucial, but only something to offer up in exchange for the right to explore - hence a non-significant relationship between *Openness to Experience* and *Attitude towards privacy*.

8.5.1.2 Influence on information security awareness

From the structural model, it is clear that Openness to Experience exhibits a statistically significant (0.283*** at p<0.01) influence on *Information security awareness*. Given that one of the awareness items states that it is a good idea to check up on privacy settings periodically and to be knowledgeable about secondary use, individuals high in Openness to Experience may also view this as an exercise in exploration. These individuals find such activities enjoyable, since it appeals to their curious nature (see Section 4.2.1). From a behavioural perspective, this result corresponds with those of Camadan et al. (2018) who found that teachers high in Openness to Experience are more likely to use new classroom technologies.

The awareness construct also included items on information privacy concerns by capturing respondent views on visibility and collection of personal information (their own and their friends). Again, these individuals' propensity for exploration and higher cognitive abilities may make them more aware, and thus more knowledgeable about the possibility that their Facebook Apps may collect their friends' personal information. In a recent study conducted by Johnston et al. (2016), they found evidence to support the exploratory tendencies of individuals high in Openness to Experience. In their study, the authors report that individuals high in Openness to Experience are more likely to commit information security policy violations if there is some observed benefit to do so. As such, one could argue that these individuals' desire to explore exceeds their fear of the negative consequences thereof, but only if it benefits them. Thus, given the significant relationship with awareness, it is plausible that they are indeed concerned about the extent that their friends could collect their personal information. This is further substantiated since individuals high in Openness to Experience carefully consider privacy concerns due to their cognitive inclinations. Together with the fact that research indicates an increase in awareness leads to an increase in the use of cognitive evaluation, it makes it possible to further argue in favour of the significance of this relationship. Although partially related, McCormac et al. (2017) also found Openness to Experience to share a positive and statistically significant relationship with information security awareness.

In summary, the desire to explore (individuals high in Openness to Experience) is likely to increase these individuals' level of awareness and knowledge of secondary use. In turn, this is likely to further raise awareness, which further raises concerns. As stated, this makes these individuals cognitively (rather than affectively) appraise privacy concerns, which further increases awareness and knowledge of Facebook App surveillance. Hence, the statistically significant relationship between *Openness to Experience* and *Information security awareness*. Notably, this relationship also exhibited the largest effect size (f^2=0.732) on *Information security awareness*. In other words, of all the personality traits *Openness to Experience* contributes the most to the explanatory power of *Information security awareness*.

8.5.1.3 Influence on social norms

As per the structural model, Openness to Experience is not significantly related to *Social norms*. This is expected, since individuals high in Openness to Experience generally avoid conforming to accepted norms. As such, they do not place much emphasis on how others think they should behave (see Section 4.2). Additionally, these individuals display an overall disregard for authority. It is thus likely that these individuals will avoid social groups, especially since social norm theory suggests authority figures (i.e., senior group members) determine which norms to adhere to (see Section 5.3). Individuals high in Openness to Experience are thus unlikely to use Facebook Apps that are recommended or used within the social group/s or community they frequent.

The direct influence of Openness to Experience is not often studied within this context. As such, there is limited recent research to support this result. For example, Lönnqvist & Itkonen (2016) found that individuals high in Openness to Experience tend to be friends with other individuals high in Openness to Experience; especially if they share the same values. Together with their non-conformist attitude, it stands to reason that a social group consisting of mostly individuals high in Openness to Experience are less likely to adhere to social norms. This naturally lends itself to Facebook, simply because these users can build a list of online friends. Given that such a list of friends most likely contains other individuals high in Openness to Experience, very little norm-driven use of Facebook Apps is likely to occur. Hence, the relationship between *Openness to Experience* and *Social norms* is not statistically significant.

8.5.2 Conscientiousness personality trait

8.5.2.1 Attitudinal influence

As illustrated in the structural model a statistically significant and positive (0.186** at $p<0.05$) relationship exists between *Conscientiousness* and *Attitude towards privacy*. Since attitude in this context largely refers to respondent views about information privacy and the use of privacy settings, such a positive relationship is to be expected. For example, personality theory suggests that individuals high in Conscientiousness are responsible and reluctantly make use of the Internet. Additionally, social media is viewed as something that detracts from achieving their goals (see Chapter 4 on characteristics of conscientious individuals); thus, contributing to the negative relationship between *Attitude towards privacy* and *Intention to use Facebook Apps*. More importantly, individuals high in Conscientiousness are cautious about the personal information they share; hence the largely positive attitude towards the use of privacy settings as per the univariate analysis.

It stands to reason that the more aware these individuals are, the more inclined they would be to use privacy settings. This, in turn, provides support for the positive relationship illustrated in the structural model. Such increased levels of awareness may also influence these individuals' intention to use Facebook Apps. Given their cautious, responsible, and risk-averse nature (see Section 4.3) a negative attitude towards intended use is thus expected and supported by the univariate results which indicated that the use of Facebook Apps is risky (as per Table 7.20).

Considering that knowledge sharing (as part of education) is not a primary use case of popular Facebook Apps (Perrin & Anderson, 2019), and individuals high in Conscientiousness are less likely to share knowledge (Hao et al., 2019), the positive relationship between *Conscientiousness* and *Attitude towards privacy* is plausible. As is the case with individuals high in Openness to Experience, an individual high in Conscientiousness may thus also see Facebook Apps (and the information shared through its use) as something that does not attribute to knowledge. For instance, this information may be viewed as too personal (i.e., something that peers and the public should not know). Importantly, *Conscientiousness* has a medium effect (f^2=0.153) on *Attitude towards privacy*. In other words, *Conscientiousness* contributes the most to the explanatory power of *Attitude towards privacy*.

8.5.2.2 Influence on information security awareness

Conscientiousness also exhibits a statistically significant and positive relationship with *Information security awareness* (0.310*** at p<0.01). Individuals high in Conscientiousness are thorough and organised (as per Section 4.2), and thus likely to check their Facebook privacy settings periodically. It is also likely that their responsible nature makes them more concerned about the fact that their Facebook Apps can access their friends' personal information. Since Codish & Ravid (2014) found individuals high in Conscientiousness to dislike leaderboards (a means to increase awareness of scores) a heightened level of concern is plausible. In other words, these individuals may view the access their friends' Facebook Apps have to their personal information as a form of leaderboard in that their friends will become more aware and knowledgeable about the Apps they use, as well as how they are used. This makes even more sense considering that many of the Facebook Apps are indeed gamified (the most popular App being Candy Crush Saga) and thus likely to possess characteristics of leaderboards. It is also quite possible that these users are not inclined to use Facebook Apps at all, since theory suggests that they view it as a distraction. All of the above may contribute to the overall negative relationship between *Information security awareness* and *Intention to use Facebook Apps*. Moreover, *Conscientiousness* has a large effect (f^2=0.353) on *Information security awareness*. Thus, contributing the second most to the explanatory power of *Information security awareness*. The results of this study are confirmed by McCormac et al. (2017) who also found Conscientiousness to exhibit a significant and positive relationship with information security awareness.

8.5.2.3 Influence on social norms

As per the structural model, there is a non-significant relationship between *Conscientiousness* and *Social norms*. In this regard, personality theory provides several characteristics which may explain this. For example, individuals high in Conscientiousness are both reluctant social media users and cautious about sharing their personal information online (see Section 4.2 and 4.3). They also tend to build relationships of high quality when they do share personal information. Together with the fact that the most popular Facebook Apps are gamified, and thus possess minimal features with which to build such relationships, it is unlikely that individuals high in Conscientiousness will use Facebook Apps intensively (or at all for that matter).

Nevertheless, there are studies which contradict the results of this study. For example, Shropshire et al. (2015) found that individuals high in Conscientiousness are likely to follow accepted norms. Other studies have also found more conscientious individuals to engender a positive perception of social media. Given that these individuals are more likely to use social media platforms, like Facebook, in a responsible and goal-oriented manner it is less likely that they are going to engage with Facebook Apps - mainly because most Apps are not focused on achieving a goal. The fact that peers and significant others are using these Facebook Apps are thus less likely to influence individuals high in Conscientiousness to also use these Apps.

8.5.3 Agreeableness personality trait

8.5.3.1 Attitudinal influence

For individuals high in Agreeableness fear exerts a significant influence on resultant behaviour (as per Section 4.3). As such, it is likely that these individuals' positive attitude towards information privacy within this context, is mainly fear-induced. Fear that their privacy settings may inadvertently leak information about their friends (Koban et al., 2018) or themselves (Shropshire et al., 2015), which may lead to psychological harm.

It is thus argued that together, both fear and concern over information privacy, drive the behaviour of individuals high in Agreeableness. This, in turn, could explain the statistically significant (0.086** at $p<0.05$) relationship between *Agreeableness* and *Attitude towards privacy* (Osatuyi, 2015). Additionally, *Agreeableness* has a medium effect ($f^2=0.113$) on *Attitude towards privacy* and thus contributes the second most to the explanatory power of *Attitude towards privacy*. Given the sensitivity towards the views of others that surround those high in Agreeableness, one also has to consider the personality traits of surrounding individuals - an aspect that is nearly impossible to gauge in this study. It is, however, possible to theorise the influence of the media. Considering the pervasive nature of mass media, and recent negative publicity regarding Facebook's misuse of personal information, these individuals are likely to have formed attitudes based on the influence of awareness and norms. Evidence to this extent is provided by Koohikamali et al. (2017), who found that Agreeableness, for both females and males, were significantly related to information privacy concerns.

Although results indicate that individuals high in Agreeableness value the use of privacy settings, excessive use may be viewed as an impediment to enjoying such benefits (Pentina et al., 2016). Furthermore, such excessive uses may also cause these individuals to question not just how useful these settings are, but also how effective they are at using them. Since this is a form of self-efficacy, which is mostly based on how knowledgeable these individuals are with regards to the use of the settings, awareness is a likely candidate for a mediated effect. For instance, the more aware these individuals are regarding the effectiveness of Facebook privacy settings, the more likely they are to self-assess its usefulness. Bansal et al. (2016) further support the latter; not only in terms of the significance of the relationship, but also its strength. For example, their study found that Agreeableness also shared a weak relationship with privacy concern in both financial and e-commerce contexts.

8.5.3.2 Influence on information security awareness

Agreeableness exhibits a non-significant relationship with *Information security awareness*. Given that agreeable individuals trust other individuals, it is plausible they are not concerned about the accessibility of their personal information. Research has also found individuals high in Agreeableness to be eager to comply with information security policies. Their trusting nature also assumes others to behave similarly (see Section 4.2). Sønderskov & Dinesen (2016) uncovered evidence that Agreeableness is significantly related to trust; specifically social and institutional trust. However, the latter study directly addressed trust whereas this study only uses it as part of a larger argument (see Section 5.2.3), and thus touches on it indirectly in the form of concerns about access to personal information. Another study conducted in Switzerland also supports the argument that individuals high in Agreeableness exhibit the propensity to trust others; even strangers (Freitag & Bauer, 2016). The findings of Pentina et al. (2016) also provides further support for the non-significant nature of this relationship. Pentina et al. (2016)'s study also found that Agreeableness is not significantly related to privacy concerns. Moreover, the results from the study were consistent for respondents from both China and the United States. Additionally, individuals high in Agreeableness tend to be overly optimistic. In this regard, some studies indicate that the relationship between optimism and Agreeableness is mediated through other psychological aspects - one being emotional intelligence (Di Fabio et al., 2018). Given that this study does not evaluate such aspects, this may further attribute to the non-significant nature of the relationship.

On the other hand, some researchers have found evidence that contradict those presented above. Koohikamali et al. (2017), for example, found that individuals high in Agreeableness are significantly concerned with the privacy of others. As outlined above, it is thus plausible that these individuals do not view safety and trust as similar concepts. At least not to the extent that an increase or reduction in trust influences the safety of their personal information. The findings of De Feyter et al. (2012) also contradicts this study's findings - albeit in a context related to academic performance. In turn, this suggests that individuals high in Agreeableness do not view knowledge within the context of Facebook as an essential behavioural influence. Because some Facebook Apps use nicknames, more agreeable individuals may view such forms of anonymity as an opportunity not to engage with knowledge acquisition, since there is less of a need to conform and trust what others are doing. Together, the above provides some evidence that the trusting nature of individuals high in Agreeableness may be the cause of the statistically non-significant relationship between *Agreeableness* and *Information security awareness*.

8.5.3.3 Influence on social norms

Agreeableness exhibits a positive and statistically significant (0.163*** at p<0.01) relationship with *Social norms*. Additionally, *Agreeableness* has a medium effect (f^2=0.216) on *Social norms* and thus contributes the second most to the explanatory power of *Social norms*. This result confirms known personality theory in that individuals high in Agreeableness tend to be concerned with what others think of their behaviour (see Section 4.2 and 4.3). They also tend to cooperate and work well within a group setting. All of which makes them more inclined to adhere to social norms.

Significant relationships between Agreeableness and norms are reported a number of other studies. For instance, Erevik et al. (2018) found individuals high in Agreeableness to be more attentive to the behaviour of others in social settings. Similarly, Stavrova & Kokkoris (2019) found these individuals to be particularly attentive to the needs of their social group. Additionally, Kim & Chock (2017) found individuals high in Agreeableness to post more group selfies. Together with the fact that these individuals are less likely to post solo selfies, it is plausible that individuals high in Agreeableness are particularly attentive to both what others are doing, as well as the perception of what they ought to do. As such, if the peers or significant others of more agreeable individuals use Facebook Apps, they are most likely also going to use these Apps. Hence the significant (and positive) relationship with *Social norms*.

8.5.4 Extraversion personality trait

8.5.4.1 Attitudinal influence

The relationship between *Extraversion* and *Attitude towards privacy* is statistically significant (-0.064** at $p<0.05$), negative and has a small effect ($f^2=0.014$) on the explanatory power of *Attitude towards privacy*. As such, individuals high in Extraversion exhibit a negative attitude towards information privacy. From the literature reviewed (Section 4.3), these individuals are more inclined to take risks and seek social interaction, regardless of other factors. Because of this, these individuals often have more Facebook friends and an inclination to be self-conscious about how they portray themselves to these friends. As such, similar to those high in Agreeableness, individuals high in Extraversion value the overall sentiment of others. Given the weak nature of the relationship and the importance they place on the views of others, it is plausible that a mediated effect through *Social norms* exists (not statistically evaluated in this study). Evidence of such a mediated effect can be found in the results of the study conducted by Riquelme & Román (2014) who established that the more extroverted individuals are, the weaker the influence on consumer trust when taking into account aspects such as perceived information privacy. Additionally, being less educated was found to further weaken the relationship. In turn, this means that the higher an individual is in Extraversion, the less concerned they are about information privacy.

Given that the relationship between *Extraversion* and *Attitude towards privacy* is negative and weak, it is plausible that most of the respondents were not excessively high in extraversion (confirmed in histogram illustrated in Figure 7.4). Such inferences are not without precedent, with several related studies making similar claims within the context of information privacy (Chen, 2011; Junglas & Spitzmuller, 2006).

Conversely, some studies have not been able to find a significant relationship between Extraversion and individuals' concern for the safety of their personal information. For instance, Pentina et al. (2016) found no significant relationship between Extraversion and information privacy concern when deciding to adopt mobile Apps. Moreover, these results remained similar for respondents from both China and the US. Considering that the items associated with privacy concerns formed part of the construct *Information security awareness*, it is also possible that the construct could mediate the relationship. However, since the bi-directional relationship between *Information security awareness* and *Attitude towards privacy* was not statistically evaluated the extent of this mediated effect cannot be determined. Given that individuals high in Extraversion are influenced by the views of their friends and peers, it is also possible that *Social norms* could mediate the relationship between *Extraversion* and *Attitude towards privacy*. Together these relationships could theoretically contribute to the weak relationship between the latter constructs.

8.5.4.2 Influence on information security awareness

As illustrated in Figure 7.9, there is no statistically significant relationship between *Extraversion* and *Information security awareness*. Since individuals high in Extraversion are more likely to engage in risky behaviour (Section 4.2), it is plausible that they do not deem it necessary to check their privacy settings periodically. The same applies when considering concerns that their friends' Facebook Apps may be able to access their personal information. Additionally, individuals high in Extraversion tend to be positive, and it is thus possible that they are overly optimistic (i.e., negative events will not affect them) and thus use the platform more intensively. Moreover, some studies found that the latter predisposes these individuals to develop a Facebook dependency (see Section 4.3). This is especially pertinent given that recent studies confirm that higher levels of Extraversion are significantly related to the increased use of Facebook (Suebsumrarn & Varma, 2019). Given that a sizeable portion of this study's respondents both use Facebook for extended periods (see Table 7.17) and have more than 400 friends, their use of Facebook might outweigh being concerned about the privacy of their personal information.

This is especially important, given that heightened levels of cortical arousal cause these individuals to require increasing levels of stimulation (i.e., through communication on Facebook, for example) (Schultz & Schultz, 2016, p.282). This makes social media platforms, like Facebook, appealing (Wilson et al., 2010). So much so, that information security awareness does not feature as a primary influence on both intended or actual behaviour. As such, in the case of individuals high in Extraversion, the cyclical relationship between knowledge and awareness (see Section 5.1.1) does not seem to influence their intention to use Facebook Apps. Any risks or adverse side-effects are merely noted, but does not result in significant behavioural change. Several other studies confirm the non-significant relationship between *Extraversion* and *Information security awareness*. For example, Shappie et al. (2019) found that Extraversion is not significantly related to cybersecurity behaviour as influenced by awareness. Cusack & Adedokun (2018) found evidence that individuals high in Extraversion are more likely to fall victim to social engineering attacks, which further suggests that they are either not as aware or ignorant if they are aware of information security threats.

However, some studies also contradict the results of this study - albeit partially. For example, Gratian et al. (2018) found individuals high in Extraversion to be particularly concerned about securing the devices used to access and store personal information. However, similar to this study, no significant relationship could be found between Extraversion and proactive awareness. Given this, it is thus plausible that individuals high in Extraversion do not view information security awareness as a significant factor within the context of Facebook Apps.

8.5.4.3 Influence on social norms

As per the structural model there is a positive and statistically significant relationship between *Extraversion* and *Social norms* (0.170*** at p<0.01). Additionally, *Extraversion* has a medium effect (f^2=0.312) on *Social norms*, but does contribute the most to the explanatory power of *Social norms*. This result is supported in the literature (see Section 4.2), since individuals high in Extraversion are generally concerned with the views and opinions of others (Devaraj et al., 2008). It is thus likely that individuals high in Extraversion would make use of Facebook Apps, if peers and significant others are also using them.

Individuals high in Extraversion also exhibit a particularly strong desire to communicate (Wolfradt & Doll, 2001), which translates to increased use of mobile devices, including Smart Phones. Together with the fact that Facebook use mostly takes place on mobile devices (Chen, 2019), it is likely that individuals high in Extraversion would also intend to use Facebook Apps; specifically in a communicative capacity. The latter forms of communication further increases the likelihood that these individuals will be influenced by the norms of their social group. Kim & Chock (2017) also found a significant relationship between individuals high in Extraversion and group selfies, suggesting that these individuals are likely to engage with social groups. This further increases the likelihood of reciprocal communication within social groups. For example, Ong et al. (2011) found that individuals high in Extraversion tend to have more Facebook friends than other personality traits.

Together with the fact that the study also found a significant relationship between the number of Facebook status updates and Extraversion, it is plausible that more communication will take place. Because individuals high in Extraversion are self-conscious, it is thus also likely that during periods of increased communication, they would compare their self-image with that of the members within their social group. As such, the communication within the social group takes place via Facebook Apps (such as Facebook Messenger), individuals high in Extraversion would likely not only be influenced by group norms, but also intend to use these Facebook Apps. Hence the significant relationship as illustrated in Figure 7.9.

8.5.5 Neuroticism personality trait

8.5.5.1 Attitudinal influence

Similar to Openness to Experience, Neuroticism's relationship with *Attitude towards privacy* is also not statistically significant. To adequately support this, one has to consider some of the characteristics that define these individuals. For example, over and above being emotionally unstable and depressed, these individuals tend to find technological change stressful (see Section 4.3). They also exhibit a general distrust of technology; specifically, technology that lends themselves to the surveillance of their behaviour. It is thus plausible that information privacy, and the settings that control it, are viewed as yet another stressful technological feature they need to deal with. Additional stress within this context is especially pertinent given that Peleg et al. (2017) found evidence to suggest that individuals high in Neuroticism judge themselves to be ineffective at managing their own security. It is thus plausible that these individuals will avoid applications like Facebook Apps; especially, those Apps that require extensive amounts of personal information. In turn, this contributes to the overall negative relationship between *Attitude towards privacy* and *Intention to use Facebook Apps*.

Neurotics are also likely to exhibit a sense of superiority when making use of social media (Wallace et al., 2017), which may indicate that they view privacy settings as an optional feature; something that does not necessarily apply to them because they may feel overly optimistic about managing the security of their personal information. The literature review also indicates that individuals high in Neuroticism do not find technology to be particularly useful (see Section 4.3). Together with their inclination to exhibit sensitivity to the certainty of sanctions (Section 6.2.4), these individuals may not find features that safeguard their personal information of any use.

Although some studies have found evidence that contradicts the findings of this study, these are not recent. Thus, given the central role of awareness (see Section 5.4) and the fact that awareness of social media and Facebook App surveillance only reached mainstream media circa 2013 (i.e., post Snowden), these results were likely shaped by other influences. This increases the difficulty in making a contemporary comparison that could be used to counter the argument that they may not have much use for privacy management features (i.e., Facebook privacy settings). Those studies that have found evidence to support the fact that neurotic individuals favour control mechanisms (similar to privacy settings,) did so within the context of compulsive shopping - a form of dependency (Wang & Yang, 2006). Given that individuals high in Neuroticism are more inclined to develop social media dependencies, and such dependencies lead to ignorance of safety features, it is possible that these settings do not feature for these individuals. Especially when making use of Facebook

Apps. Hence, the non-significant relationship between *Neuroticism* and *Attitude towards privacy*.

8.5.5.2 Influence on information security awareness

Like *Openness to Experience*, *Neuroticism* also exhibits a statistically significant relationship with *Information security awareness* (0.167*** at $p<0.01$). Additionally, *Neuroticism* has a medium effect ($f^2=0.216$) on *Information security awareness*. There are several characteristics of Neuroticism which could be used to argue in favour of the latter. For example, individuals high in Neuroticism are typically negative and distrustful of technology. They also tend to be cautious when sharing personal information (see Section 4.2). It is thus plausible that these characteristics result in higher levels of concern regarding their friends having access to their personal information. The same applies to periodically checking on Facebook privacy settings in that they might think, or be worried that Facebook has changed the functionality of the privacy settings. The same paranoid and worrisome characteristics also play into how important it is for them to be knowledgeable about secondary use of personal information. Given that this study's respondents were mostly under the age of 34, and research has shown younger individuals to use Facebook more intensively (see Section 4.3), it makes these individuals more likely to develop a Facebook dependency (Hughes et al., 2012).

Together with their propensity to depend on Facebook, their need to control their information could also explain a heightened level of concern with regards to the accessibility of their personal information. Moreover, the fact that individuals high in Neuroticism are generally selfish Internet users (Section 4.2) may explain the relationship strength. This stems from the fact that not all the items that evaluated respondents' concern over access to their personal information were from the perspective of the information owner. For example, some items asked respondents about their level of concern if they can access their friends' personal information. Given the selfish nature of individuals high in Neuroticism, this would not likely concern them; thus, lowering the overall concern as evaluated by those items.

Unlike this study, Gratian et al. (2018) found no significant relationship between Neuroticism and proactive awareness. This is an important finding given that the latter study's definition of proactive awareness includes aspects such as caution when sharing personal information. Upon closer inspection, few (if any) of the items in the study directly address personal information, which may explain the difference in results. Similarly, Pentina et al. (2016) also found no significant relationship between Neuroticism and privacy concerns. These results were confirmed for both Chinese and US respondents. It is worth noting that this study focused only on millenials and the use of specific information sensitive Apps. It is thus only representative within a similar context. More specifically, McCormac et al. (2017) found information security awareness to be positively related to emotional stability (i.e., individuals low in Neuroticism). Although these findings also contradict those of the current study, it is worth noting that they made use of the Human Aspects of Information Security Questionnaire (HAIS-Q), which measures information security awareness across seven domains with social media only forming one part thereof. Moreover, only one of the items (item 79) within the social media domain was deemed useful within the context of this study. This complicates matters when directly comparing results in this manner.

8.5.5.3 Influence on social norms

As per the structural model, there is a non-significant relationship between *Neuroticism* and *Social norms*. This result contradicts the literature with several studies suggesting that their insecure nature causes them to emphasise the opinions of others in terms of how they should behave (Bansal et al., 2010; Zhang, 2006). Norm-based influences are thus likely to affect these individuals (see Section 4.2). However, considering that individuals high in Neuroticism are distrustful of technology, it is plausible that they similarly view Facebook Apps. For example, in a recent study, it was found that Neuroticism had no significant relationship with phubbing (ignoring a real-life conversation while using your Smart Phone), nor with fear of missing out (FOMO) (Balta et al., 2018). This suggests that individuals high in Neuroticism are not as concerned with what their peers (and others) are doing, which may suggest that they are also not concerned with what others are doing on social media (Instagram in this case). At least not to the extent that they would consider ignoring real-life conversations instead of following their peers online.

In another study on Facebook-based virtual endorsement, individuals with a propensity to be influenced by subjective norms were found to *like* comments and posts simply because they wish to please others (Lee et al., 2016). Given that individuals high in Neuroticism tend to use the Internet selfishly (see Section 4.2), it is unlikely that subjective norms would influence them in the latter context. This is especially pertinent considering that the use of a Facebook App within a social group could be viewed as a form of norm-based endorsement. In other words, if the majority of the group or community uses a specific Facebook App, other members are likely to accept that the App has been endorsed - albeit informally. Given this argument, it is thus likely that social norms would significantly influence individuals high in Neuroticism to intend making use of Facebook Apps.

8.5.6 Vulnerability of the personality traits

Table 8.1 provides a summary of the personality-based discussion by not only indicating each personality trait's core characteristics, but also how vulnerable these personality traits are, given the statistical results illustrated in the structural model. For example, individuals high in Extraversion are the most vulnerable, since these individuals are influenced by peers, significant others, and generally enact risky behaviour. In the latter example, the influence of *Extraversion* has a medium effect (Cohen, 1988) on *Social norms*. In other words, if others are using Facebook Apps in a risky manner so will individuals high in Extraversion. This is compounded by the fact that the structural model indicates that these individuals exhibit a negative attitude towards privacy. Conversely, individuals high in Conscientiousness are the least vulnerable, since they are not only more aware of information security (a large effect on *Information security awareness*), but also exhibit a positive attitude towards privacy (also a large effect).

8.6 Information security awareness in context

Thus far the discussions have mainly focused on specific and somewhat isolated relationships between the various model constructs. Subsequently, the problem statement and its applicability within this context have not been addressed in specific terms. It is the objective of this section to discuss the problem statement and implications of Chapter 3, by not focusing on the research model constructs, but rather on the latent aspects that have emerged as the study unfolded. Importantly, this section visually illustrates (see Figure 8.1) this study's

Table 8.1: Each personality trait's level of vulnerability

	Openness to Experience	Conscientiousness	Extraversion	Agreeableness	Neuroticism
Core characteristics	*Non-conformist, intellectual and inquisitive.*	*Emotionally stable, goal-oriented and not easily influenced.*	*Sociable, easily influenced and open to risky behaviour.*	*Self-conscious, easily influenced and trusting.*	*Emotionally unstable, distrustful and negative.*
ATP	0.056^{ns} (f^2=0.098)	0.186** (f^2=0.153)	-0.064** (f^2=0.014)	0.086** (f^2=0.113)	0.053^{ns}
AWA	0.283*** (f^2=0.732)	0.310*** (f^2=0.353)	-0.044^{ns}	-0.003^{ns}	0.167*** (f^2=0.216)
SN	-0.047^{ns}	-0.025^{ns}	0.170*** (f^2=0.312)	0.163*** (f^2=0.216)	0.077^{ns}
Vulnerability level	*Positive relationship with information security awareness (**Thus, less vulnerable. VL = 2**).*	*Positive relationship with information security awareness. Positive attitude towards privacy (**Least vulnerable. VL = 1**).*	*Susceptible to influence of norms and exhibits negative attitude towards privacy (**Most vulnerable. VL = 5**).*	*Susceptible to influence of norms and exhibits a positive attitude towards privacy (**More vulnerable; especially if influenced by peers. VL = 4**).*	*Positive relationship with information security awareness (**Thus, less vulnerable. VL = 3**).*

*** = significant at p<0.01
** = significant at p<0.05
ns = not significant

understanding of the interplay between these aspects, starting with an example-driven explanation of Figure 8.1.

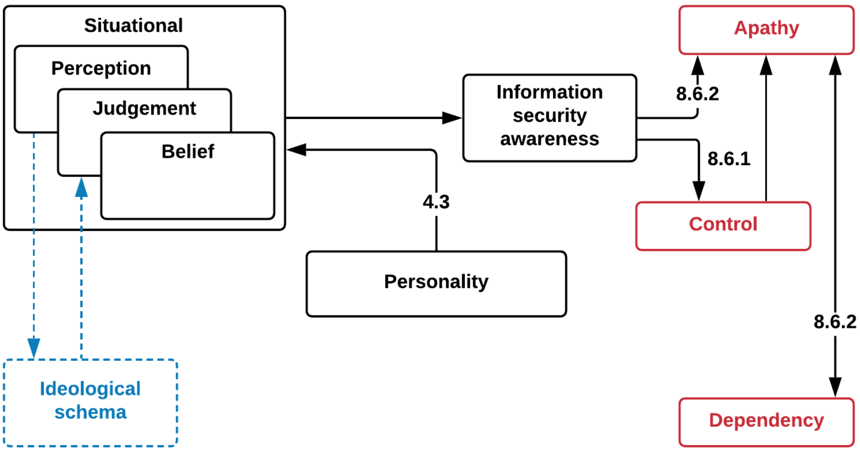


Figure 8.1: Information security awareness in the context of this study

Throughout this study, several diagrams were used to illustrate how the study context and personality theory integrates with the Theory of Planned Behaviour (TPB). Within these illustrations, an individual's perception, judgement, and beliefs are illustrated as fundamental processes that shape the stimuli before being integrated into the TPB. Together, these processes not only provide the means to shape stimuli, but also determine that which an individual becomes aware of. For example, stimuli are first perceived and then judged, based on an individual's existing ideological beliefs and values (Van Dijk, 1998). Depending on the individual's existing ideological beliefs, the judged perceptions are either incorporated into their ideological schema or rejected. For example, as an individual becomes aware of Facebook App surveillance, their ideological beliefs may conflict with such practices.

To further illustrate this, consider the Snowden revelations from the perspective of Edward Snowden. For Snowden, government surveillance (of which social media is a part, as per Chapters 1 and 3) is a problem for society at large, simply because his beliefs of what constitutes patriotism declare this to be unjust (Snowden, 2013). Nevertheless, Snowden was also exposed to specific situational conditions - one being the terrorist attacks on September 11, 2001. At the time, his beliefs of government surveillance were the result of judged perceptions based on these attacks. In turn, this, together with those beliefs and values that form part of his existing ideological schema, would have led to the formation of a sentiment which ultimately influenced his attitude towards such terror attacks.

Following this, the then National Security Agency (NSA) director (Michael Hayden) was instructed to develop a means to pro-actively eliminate similar attacks going forward. This resulted in the creation of the PRISM surveillance programme. Because Snowden disagreed with the extent to which government surveillance was taking place (based on a judged perception of these NSA programmes), he changed his attitude towards such surveillance practices.

The same processes illustrated in Figure 8.1 also apply to users of Facebook Apps, and although some of this has been argued in the literature review, it has not been fully integrated with information security awareness. Specifically, those latent aspects which relate to both awareness and intended use of Facebook Apps.

8.6.1 Privacy control and concerns

Every individual has a choice as to whether they will make use of social media; specifically Facebook Apps in this context. Such choices are controlled by two aspects, namely that which an individual consists of (their personality and genetic make-up), as well as the situations these individuals are faced with. Controlling either one of these is vital if the objective is to influence choice or behaviour as argued in this study (Martinez, 2017).

It is not possible to control an individual's personality, but it is possible to influence (if not control) situations. Such control requires mechanisms to shape the possibilities when using social media or Facebook Apps. Here, possibilities refer to that which is permissible and not permissible. Within the context of this study, this refers to those pieces of personal information that are always available and those that are not. Such coercive forms of power not only limit possibilities, but also maintain a sense of inequality in that the free services provided by social media platforms come at a price. The price is personal information to be shared in order to use the App. At first, this may seem like a fair trade. The user gains access to services, and the social media platform (like Facebook) gains access to their personal information. However, the platform has access to a never-ending production line of commodities in the form of shared information; information that is continually being created or updated by users. As such, the *fair trade* is not so fair, requiring increasing amounts of coercive power in the form of limiting choices (Martinez, 2017, pp.95-98). The more unequal the fair trade is, the more coercion is required.

In the case of Facebook and Facebook Apps, such control of choices, and to some extent, coercion is performed by privacy settings and legal agreements. Facebook privacy settings have become increasingly complex. The fact that Facebook's user base continues to grow (more to commodify) lends credence to the increasing amounts of power required to uphold the status quo. The same holds for the legal statements users have to agree with before they are allowed to use the platform. These forms of coercion make it difficult for users to understand the nature of the unequal *fair trade*.

It is thus possible for Facebook to use this unequal partnership to shape the identity of users, or at least nudge them into directions so that they think they have shaped their identity on their own. In a way they become what Cambridge Analytica would call *persuadeables*; a set of shared beliefs that are open to suggestion and coercian. In this study's structural model those individuals are more vulnerable. Shaping identities in this manner makes it possible for the users to feel as if they are in control when, in fact, they are merely channelled to use the platform and Apps in certain ways. As stated in Chapter 1, Facebook and other social media platforms have long since realised that,

> *"The shaping of a person's identity - their beliefs, values, fears and desires - can be an extremely effective form of control." (Martinez, 2017, p.95)*

So, although Facebook makes privacy protection tools (like Privacy Shortcuts and the Privacy Checkup tool) available to those users users who are aware and concerned, these are likely to also influence forms of shaping and channelling resultant use (and the information available). Recall that some users are not fully aware of the extent that their personal information is misused. To some extent, this has taken place because the media and press have been used as mechanisms to shape beliefs that make users accept these forms of coercion willingly or apathetically (see below). This ties directly into the thesis problem statement. For example, common sense dictates that if an individual is aware of the risks to their personal information, they will cease using Facebook Apps. However, this is not necessarily the case, with many users continuing to use Facebook and thus also Facebook Apps; even after becoming aware of the extent to which such misuses take place. Thus there are other reasons why users use Facebook Apps, which transcend their logical usage.

8.6.2 Apathetic dependence and privacy

One aspect which may transcend the influence of both personality and awareness on the intended use of Facebook Apps is apathy. Specifically, apathy towards information privacy as a function of the ever-increasing dependence on information and the consumption thereof (see Section 3.4.1). Facebook Apps being one such facilitating mechanism. In an effort to exude a sensible approach to information privacy some (if not all) individuals often intend to enact privacy-protective behaviour, but fail to do so in reality. This (referred to as the Privacy Paradox) has not only been studied in and of itself (Kokolakis, 2017) but has also been linked to apathetic use of social media. For example, Hargittai & Marwick (2016) states that a lack of awareness (of risks and knowledge to protect information) has been put forward as a possible reason why this paradox exists.

However, there is possibly another reason; one which allows for a different appraisal of information security awareness in this context, namely, social media and information dependence. Increasingly, individuals are not only using social media for pleasure, but also to function within modern society. Young individuals primarily use social media to search for employment, educate themselves and socialise. Hargittai & Marwick (2016) found that most individuals below the age of 35 are more concerned with social risks when disclosing personal information than those risks posed by social media corporates - even though they are aware of the potential risks posed by social media corporates like Facebook.

To ameliorate these concerns, some individuals classify their information into that which is sensitive (credit card numbers, health information) and the rest, such as browsing histories, age, and gender. However, even amidst such classification, many users remain apathetic, mainly because there is no viable alternative. If for example, an individual wishes to circumvent Facebook App surveillance, they would have to stop using Facebook Apps. However, since many of these Apps are used to communicate and feel a sense of belonging (see Section 4.4), it is unlikely that this will actually take place. This is illustrated in Figure 8.1, as the relationship between individuals' dependence on Facebook Apps and apathy. The more apathetic these individuals become in relation to their personal information, the more it becomes accepted and commonplace to use these Apps. In turn, this increases their dependence on these Facebook Apps. For example, users of these Apps may comment that they have been using a specific App (Facebook Messenger for example) for an extended period of time and now depend on it to communicate with their friends and family.

Apathetic dependency also applies to the communicative relationships that rely on significant others and peers of Facebook users. For example, from the literature, it is known that friends have at least some access to each other's personal information when using Facebook Apps. Facebook users are thus also dependent on how their Facebook friends configure their privacy settings. Not using Facebook or Facebook Apps because of this is most often deemed unrealistic. Individuals are thus confronted with the same ontological dilemma referred to in Chapter 3.

Raised awareness according to Hargittai & Marwick (2016) is unlikely to change this, and so the cycle continues. These users may eventually move to another App, which more often than not works in a similar manner, simply because it is convenient for a Facebook App developer to outsource an App's authentication to Facebook (i.e., using Facebook Connect). Outsourcing the authentication is also lucrative to both Facebook and the Facebook App developer who then exchange personal information. For example, the App has limited access to the user's Facebook profile, and Facebook is able to ascertain which Apps the user is using and when. Some Apps even allow users to access their Wi-Fi routers via a vendor-provided Facebook App.

Accessing Facebook Apps in this manner not only increases the convenience of doing so, but also facilitates increased access, which, as discussed, leads to an increase in a dependence on Facebook Apps. As before, apathy remains but almost becomes something akin to Marx's commodity fetishism (Fuchs, 2015) in that individuals assume that the privacy landscape (in terms of the App's access to personal information) has always been this way. In other words, the exchange of commodities (in this case information) ignores the human aspect (as prosumer and consumer) of the market exchange between the capitalist (Facebook in this context) and the worker (Facebook user); so much so, that the personal information being exchanged takes on a life of its own. Such an objective view of information as a commodity ignores the context in which it was produced. This means that personal information is increasingly harvested from varied sources through varied mechanisms (one being Facebook Apps) to produce a commodity, which in all actuality has no intrinsic value outside the information economy.

All of the above makes it easier for corporates to justify having more access to personal information rendering the *soft sell* alluded to in Chapter 3 as something that is not even required. In turn, the use of Facebook Apps (and associated surveillance of personal information) has become the norm, in so far that most individuals are either aware of such practices, but apathetically dependent or completely unaware that these Apps are performing such forms of surveillance.

8.7 Summary

This chapter discussed the theoretical implications of this study's results by providing evidence as to why the structural model's relationships are either statistically significant or not statistically significant. In particular, the extent to which each of the model constructs influences an individual's intent to use Facebook Apps. The latter included explanations as to how each of the Big Five personality traits influence the constructs *Attitude towards privacy*, *Social norms* and *Information security awareness*. In this regard, results indicate that of the 15 relationships between the five personality traits and the aforementioned constructs, seven are not statistically significant, and eight are statistically significant. Either way, sufficient evidence is provided to explain the significance of these relationships with some indication as to which personality traits are more vulnerable to Facebook App surveillance (see Table 8.1). This chapter also discussed the results within the context of the thesis problem statement, by putting forward a conceptual diagram. The problem-centric discussion focused on explaining the relationships between information security awareness, apathy, dependence, and control, as well as information privacy. Together these relationships explain the various dimensions one has to consider when theorising the extent to which individuals are aware of Facebook Apps surveillance. The following chapter provides a complete overview of this study in the form of a retrospective conclusion.

Chapter 9

CONCLUSION

> "Capitalist production, therefore, develops technology, and the combining together of various processes into a social whole, only by tapping the original sources of all wealth-the soil and the labourer."
>
> — Karl Marx

This chapter aims to provide an overview of the study, with a specific focus on how it contributes to this body of knowledge, while addressing the research questions and problem statement. Firstly, a retrospective overview is provided, followed by a discussion on the methodological approach used. Building on the results obtained, the following section provides a clear outline as to how this study's research questions have been addressed. Next, the study's contribution is discussed, with a specific focus on the relevance of the results; specifically concerning the field of behavioural information security. Following this, both the limitations and areas of future research are outlined.

9.1 Overview of thesis problem

Facebook is currently being used by over 2 billion users daily, which makes it an attractive platform to use for targeted advertising, explicitly based on traits and personal preferences (Pew Research Center, 2019a). This is especially pertinent given that Facebook has access to specific demographic information such as a user's age and gender. However, targeted advertising only accounts for some of the use cases of Facebook users' personal information. For example, personal information and real-time usage statistics are knowingly funnelled to intelligence agencies such as the National Security Agency (Hayden, 2014; Snowden, 2016, 2013) as part of supposed anti-terror campaigns. Moreover, several device manufacturers have also been given privileged access to Facebook's developer platform (Leetaru, 2018). In turn, this allows these manufacturers to create Apps that could potentially access Facebook-based personal information beyond that which users are aware of.

Specific incidents where personal information was used beyond that which users are aware of, includes the voter-profiling conducted by Cambridge Analytica (DigitalWatch, 2018). Importantly, the latter incident made use of data collected via a Facebook App called *thisismydigitallife*, which users thought was used only to determine their personality traits. However, unknowingly this App also had access to these users' Facebook friends' personal information. Once discovered, the incident was not only made public to raise awareness in this regard, but also resulted in the banning of several Facebook Apps that were found to have extensive access to users' personal information. Notwithstanding the increasing amount of media reports about Facebook's disregard for the privacy of their users' personal information, many users continue using the platform and associated Apps (Perrin & Anderson, 2019). A recent survey conducted by the Pew Research Center confirms that 69% of United States citizens still use Facebook (Pew Research Center, 2019a). Given the brief discussion above, the problem statement addressed in this study is as follows:

> *Facebook users are unaware of the trait-based analyses and subsequent misuse of the personal information gathered when making use of Facebook Apps.*

To further investigate this problem statement and its related effects, several studies have focused on either the Facebook Apps themselves (Symeonidis et al., 2018), transactional privacy when using Apps (Choi & Land, 2016), privacy risks (Farnden et al., 2015), privacy concerns when using Apps (Golbeck & Mauriello, 2016; Wisniewski et al., 2015), and the relationship between users' age and privacy management (Kezer et al., 2016). However, few (if any) have investigated the above by also focusing on the influence of personality traits; specifically with regard to intended use, given the influence of both personality and information security awareness.

9.2 Research questions revisited

From the previous section, it follows that the objective of this study was to develop a surveillance model centred on the intended use of Facebook Apps, given users' awareness as to the extent to which such surveillance is taking place. To achieve this, four research sub-questions had to be answered; all of which focused on the extent to which the research model constructs influence respondents behaviour. Together, these four sub-questions answered the following main research question:

> **Main Question.** *To what extent does the behaviour of certain Facebook users influence their use of Facebook Apps, given the misuse of personal information gathered through these Apps?*

The following provides a summary as to how the sub-questions were answered:

- **Question One.** *To what extent does a Facebook user's attitude towards information privacy influence their intention to use Facebook Apps?* This research question corresponds to the first proposition (P1) which states that; *An individual's attitude towards privacy will influence their intention to use Facebook Apps.* As per the structural model (Figure 1.1) this study found that a Facebook user's attitude towards privacy is negatively related (-0.141** at $p<0.05$) to their intention to use Facebook Apps. In other words the more positive a user's attitude towards privacy is, the less likely they are to continue using Facebook Apps. Having said this, this relationship has a small effect on the dependent variable *Intention to use Facebook Apps*.

- **Question Two.** *To what extent does information security awareness influence a Facebook user's intention to use Facebook Apps?* This research question corresponds to the second proposition (P2), which states that; *An individual's information security awareness of Facebook App surveillance will influence their intention to use Facebook Apps.* In this regard, it was found that a Facebook user's information security awareness is statistically significant and negatively related (-0.174*** at $p<0.01$) to their intention to use Facebook

Apps. In other words, the more aware and concerned a Facebook user is about Facebook App surveillance, the less they intend to use Facebook Apps. This relationship exhibited a medium effect on the dependent variable *Intention to use Facebook Apps*.

- **Question Three.** *To what extent does social norms influence a Facebook user's intention to use Facebook Apps?* This research question corresponds to the third proposition (P3), which states that; *Social norms will influence an individual's intention to use Facebook Apps.* To address this question this study found that social norms is positively related (0.124*** at p<0.01) to Facebook users' intention to use Facebook Apps. In other words, the subjective and descriptive behaviour (i.e., social norms in this context) of other individuals within a Facebook user's circle of influence has a statistically significant influence (with a medium effect) on their intention to also use Facebook Apps.

- **Question Four.** *To what extent does a Facebook user's personality traits influence their behaviour towards the intended use of Facebook Apps?* This research question corresponds to the fourth proposition (P4), stating that; *An individual's personality will influence their intention to use Facebook Apps.* As illustrated by the structural model, this study found that all the personality traits influence at least one of either *Attitude towards privacy*, *Social norms* or *Information security awareness* to a significant extent. More specifically, it was established that,

  – *Openness to Experience* significantly (0.283*** at p<0.01) influence *Information security awareness* with a large effect on the explanatory power of *Information security awareness*.

  – *Agreeableness* significantly influence both *Attitude towards privacy* (0.086** at p<0.05) and *Social norms* (0.163*** at p<0.01) with a small and medium effect on the explanatory power of *Attitude towards privacy* and *Social norms*, respectively.

  – *Extraversion* significantly influence both *Attitude towards privacy* (-0.064** at p<0.05) and *Social norms* (0.170*** at p<0.01) with a small and medium effect on the explanatory power of *Attitude towards privacy* and *Social norms*, respectively.

  – *Neuroticism* significantly (0.167*** at p<0.01) influence *Information security awareness* with a medium effect on the explanatory power of *Information security awareness*.

  - *Conscientiousness* significantly influence both *Attitude towards privacy* (0.186** at p<0.05) and *Information security awareness* (0.310*** at p<0.01) with a large effect on the explanatory power of both the latter constructs.

    The remaining relationships were found to be non-significant. As such, they do not significantly influence *Attitude towards privacy*, *Social norms* and *Information security awareness*.

9.3 Methodological approach

This study was conducted within the post-positivist paradigm and employed a survey methodology for both the secondary and primary data collection. Secondary data was used to inductively develop four propositions, based on the Theory of Planned Behaviour. The secondary data was collected using a scoping review and analysed using Atlas.ti to assist with the process of content analysis. This scoping review consisted of three phases resulting the creation of,

- A first phase of secondary data analysis, which resulted in 8 code groups (i.e., main themes) comprising 209 codes. In turn, these 209 codes summarised 2535 quotations.
- A second phase of secondary data analysis, which resulted in 10 code groups comprising 17 codes. In turn, these codes were associated with 105 quotations.
- A third phase of secondary data analysis, which resulted in 16 code groups (i.e., main themes) comprising 58 codes. In turn, these 58 codes summarised 443 quotations.

Following this, a number of items and constructs were identified (or created), based on the results of the secondary data analysis. Additionally, where possible, existing items were used. For example, to evaluate the respondents' personality traits an established 44 item scale (the Big Five Inventory) was included in the questionnaire (John & Srivastava, 1999). The initial questionnaire was pilot tested between 9 December 2018 and 11 December 2018. During this time, a total of 21 responses (N=21) were collected and used to conduct initial validity and reliability testing.

After making several minor amendments, the final questionnaire was administered to users registered on Amazon Mechanical Turk. To qualify, participants had to be citizens of the United States, over the age of 18 and active Facebook users. Using the final questionnaire, data collection took place between 24 January 2019 and 22 February 2019. Although the process of data collection resulted in the collection of 651 responses (N=651), several of these were deemed unsuitable. Suitability was based on the following criteria:

- The response had to be complete,
- Both *attention trap questions* had to be correctly answered,
- Responses completed in less than five minutes were discarded, and
- Their social desirability scores had to be lower than those of Snyman et al. (2017).

After applying these criteria, a total of 537 (N=537) usable responses remained, forming the basis of any subsequent analyses. Two approaches were followed to analyse the primary data. Firstly, a univariate process of analysis was used to summarise the data. This was followed by a process of multivariate analysis (employing Partial Least Squares path modelling) culminating in the development of a structural model (see Figure 1.1).

9.4 Contribution

This study contributes to known theory on several fronts. Firstly, it includes the construct *Social norms* comprising both subjective and descriptive norms. Few (if any) studies have evaluated the influence of both these norms within a surveillance context. Secondly, the construct *Information security awareness* was substituted for *Perceived Behavioural Control* (as per original TPB) and argued as a central - albeit theoretical - component of both the subsidiation process and a means to control the acquisition of knowledge. This study also further expanded upon the TPB, by including the personality traits as defined within the Big Five.

Additionally, this study also contributes theoretically by indicating which personality traits are the most vulnerable to Facebook App surveillance (see Table 9.1). For example, individuals high in Extraversion were found to be particularly vulnerable followed by individuals high in Agreeableness. As such, these individuals should be encouraged to use Facebook Apps in a responsible manner, and to take care when disclosing personal information when using these Apps. This study also contributed from a holistic perspective by

Table 9.1: Summary of the personality trait's level of vulnerability

	Openness to Experience	**Conscientiousness**	**Extraversion**	**Agreeableness**	**Neuroticism**
Core characteristics	*Non-conformist, intellectual and inquisitive.*	*Emotionally stable, goal-oriented and not easily influenced.*	*Sociable, easily influenced and open to risky behaviour.*	*Self-conscious, easily influenced and trusting.*	*Emotionally unstable, distrustful and negative.*
Vulnerability	*Positive relationship with information security awareness (**Thus, less vulnerable**).*	*Positive relationship with information security awareness. Positive attitude towards privacy (**Least vulnerable**).*	*Susceptible to influence of norms and exhibits negative attitude towards privacy (**Most vulnerable**).*	*Susceptible to influence of norms and exhibits a positive attitude towards privacy (**More vulnerable; especially if influenced by peers**).*	*Positive relationship with information security awareness (**Thus, less vulnerable**).*
Vulnerability level	**2**	**1**	**5**	**4**	**3**

evaluating the proposed research model using Structural Equation Modelling within the context of Facebook Apps; an area not explored using research of this nature.

9.5 Study limitations

There are several limitations that need to be acknowledged. Firstly, the process of multivariate analysis and the resultant structural model did not take all the relationships of the Theory of Planned Behaviour into account (as indicated by blue dotted lines in Figure 1.1). It is thus possible that some of the estimated path coefficients could have changed, given that *Attitude towards privacy*, *Information security awareness* and *Social norms* could act as mediators when these relationships are statistically evaluated. Secondly, data was only collected from United States citizens registered on Amazon Mechanical Turk. In turn, this makes it difficult (if not impossible) to generalise this study's findings to other countries and population groups. Thirdly, some of the constructs - specifically *Information security awareness* - are evaluated by items that may have produced more robust results if they were evaluated separately. For example, some of the items of this construct (although related) are aimed at information privacy concerns, whereas others are focused on Facebook privacy settings. The study is further limited in that it only used a single large-scale survey to collect data, which was subsequently used to evaluate the propositions. Additional follow-up interviews could have better explained why respondents chose specific options in the questionnaire.

9.6 Areas of future research

During the course of this study, several areas of future research emerged. Firstly, the research model could be expanded by including constructs that evaluate concepts such as information privacy control (Facebook privacy settings), apathy towards information privacy, past experience, and Facebook dependency. Specific areas that come to mind are the Facebook privacy settings together with the tools that supplement its use (i.e., Privacy Checkup tool, Timeline Review, and Privacy Shortcuts). To understand whether users are knowledgeable of threats, risks, and information security awareness is, future models could also include aspects relating to self-efficacy.

Given that there are a multitude of Facebook Apps, it would be beneficial to ask respondents which Apps they use the most. Furthermore, it is suggested that researchers provide respondents with a list of popular categories to choose from. Such additional levels of detail could be used to investigate the extent that specific App types influence use. For example, it will become possible to understand which categories of Facebook Apps users consider riskier to use.

Future research could also include constructs to address risk perception; possibly even modelling the various personality traits as moderators of the relationship between risk perception, risk propensity, and attitude towards privacy. In order to contribute in a more practical manner, future research could also adopt either a mixed or experimental-only approach. For example, in a mixed approach, researchers could create and administer a questionnaire followed by a series of interviews to better understand the results. In an experimental only study, eye-tracking software could be used to understand how Facebook users visually interact with the privacy settings and its supplemental tools. From a personality perspective, future research could also focus on other personality models (i.e., HEXACO).

9.7 Summary

This study set out to empirically evaluate the influence of a Facebook user's personality on their intention to use Facebook Apps. During this process, it also evaluated the influence of these users' attitude towards the privacy of the personal information, social norms, and information security awareness as intermediary components that also influence behaviour. Chapter 1 provided the necessary background that led up to the problem statement, which centres on the lack of awareness of the extent that Facebook users' personal information is misused. This is followed by four research questions aligned with some of the constructs prescribed by the Theory of Planned Behaviour. An outline of the study objectives is provided, focusing on the development of a personality-based Facebook surveillance model. The methodological approach is outlined next followed by a brief discussion on this study's contribution. Chapter 1 concludes with a section on the ethical considerations and thesis outline.

Chapter 2 provides a detailed discussion of the methodological approach and the research design of this study. It specifically focused on the adopted paradigm providing proper motivation as to why this made use of a post-positivist approach. This study's approach to theory development was discussed next followed by a brief discussion of this study's methodological strategy, namely, survey methodology. The research instruments (pilot and final questionnaires) were discussed, including a brief section on addressing measurement errors. This was followed by a discussion of the methods and means of data collection. This section included detailed discussions as to how the secondary data was collected and inductively analysed. The chapter concluded with a discussion on the statistical methods of analysis which were used to analyse the primary data.

Chapter 3 provided the reader with a detailed discussion of the surveillance of data. The discussion was explicitly focused on providing sufficient evidence to argue that although these surveillance practices were mostly benign, they evolved into instruments of capital accumulation in the late 90s. Social media and its role in the latter surveillance practices were discussed next, culminating in literary support for this study's problem statement in that individuals have become dependent on information. So much so, that the average person is likely not to implement privacy-protective behaviour simply because they are unaware of the extent that such surveillance takes place. The chapter concluded with a discussion on how social media corporates exploit individuals' basic desire to communicate and develop on a psychosocial level. In Chapter 4, a detailed discussion on the behavioural influence of an individual's personality was provided. The chapter started with a broad overview of personality theory progressing towards a discussion on specific personality models, such as the Big Five used in this study. This was followed by a discussion of all the personality traits within the Big Five, with a particular focus on their characteristics and behavioural influence. The chapter concluded with a brief outline as to how social media corporates exploit their users' individual differences.

Chapter 5's discussions were focused on the behavioural influence of attitude, social norms, and awareness. It started with a theoretical discussion focused on attitude formation and change, followed an outline as to how this study has integrated the construct *Attitude towards privacy* into the Theory of Planned Behaviour. Within this section it makes specific reference to the process of subsidiation, which outlines how an individual's personality influences their attitude. This is followed by a theoretical discussion of social norms as well as its integration within the TPB. This discussion also included elements relating to those components that constitute social norms in this context, such as subjective and descriptive norms. The chapter concludes with a discussion of information security awareness, its theoretical integration within this context, as well as its behavioural influence. In Chapter 6, additional evidence was provided as to the behavioural influence of attitude, social norms, awareness, and personality so as to provide additional support for this study's propositions. This chapter also formally stated each of the four propositions transposed onto a conceptual (i.e., in propositional form) version of this study's research model.

Chapter 7 presented the survey results of both the pilot and final study. This included the results of both the univariate (descriptive) and multivariate analyses. This multivariate analysis employed Partial Least Squares (PLS) path modelling, resulting in the development of both a measurement and structural model. The chapter concluded by presenting the path estimates, effect sizes, explanatory power and predictive relevance of the structural model. Limited univariate results were discussed in Chapter 8, which focused mostly on a discussion of the multivariate results presented in Chapter 7. In this regard, each of the relationships (paths) illustrated by the structural model were discussed by providing evidence to support either why the relationship is not statistically significant or why it is statistically significant. Where appropriate such evidence was obtained by making reference to this study's literature review, or by citing additional sources from a variety of disciplines. Chapter 8 concluded with two sections focused on the interplay between an individual's personality traits, information security awareness, apathetic dependence, information privacy, as well as privacy control and concerns.

REFERENCES

Ab Hamid, M., Sami, W., & Sidek, M. M. (2017). Discriminant validity assessment: Use of Fornell & Larcker criterion versus HTMT criterion. *Journal of Physics: Conference Series*, *890*(1), 1–5.

Abbas, R., Michael, K., & Michael, M. (2015). Using a social-ethical framework to evaluate location-based services in an Internet of Things world. *International Review of Information Ethics*, *22*(12), 42–73.

Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211.

Ajzen, I. (2005). *Attitudes, personality, and behavior*. New York, United States of America: McGraw-Hill Education.

Albrechtslund, A. (2008). Online social networking as participatory surveillance. *First Monday*, *13*(3).

Allport, G. W. (1931). What is a trait of personality? *The Journal of Abnormal and Social Psychology*, *25*(4), 368.

Altman, D. G. & Bland, J. M. (2005). Standard deviations and standard errors. *BMJ*, *331*(7521), 903.

Amankwa, E., Loock, M., & Kritzinger, E. (2018). Establishing information security policy compliance culture in organizations. *Information & Computer Security*, *26*(4), 420–436.

Amichai-Hamburger, Y. & Ben-Artzi, E. (2003). Loneliness and Internet use. *Computers in Human Behavior*, *19*(1), 71–80.

Amichai-Hamburger, Y. & Vinitzky, G. (2010). Social network use and personality. *Computers in Human Behavior*, *26*(6), 1289–1295.

Anderson, S., Hamilton, K., & Tonner, A. (2016). Social labour: Exploring work in consumption. *Marketing Theory*, *16*(3), 383–400.

Andrejevic, M. (2007). *iSpy: Surveillance and power in the interactive era*. Lawrence, United States of America: University Press of Kansas Lawrence.

Apostolou, G. L. (1988). Threat to privacy: The federal government's use of personal information in the new communication environment. *Telematics and Informatics*, *5*(4), 451–459.

Araujo, T., Neijens, P., & Vliegenthart, R. (2017). Getting the word out on Twitter: The role of influentials, information brokers and strong ties in building word-of-mouth for brands. *International Journal of Advertising*, *36*(3), 496–513.

Asur, S. & Huberman, B. A. (2010). Predicting the future with social media. In *Proceedings of the 2010 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology*, (pp. 492–499). IEEE.

Baker, R., Dickinson, R., & Hollander, S. (1986). Big brother 1994: Marketing data and the IRS. *Journal of Public Policy & Marketing*, *5*(1), 227–242.

Ball, R., Robb, M., Anderson, S., & Dal Pan, G. (2016). The FDA's sentinel initiative—A comprehensive approach to medical product surveillance. *Clinical Pharmacology & Therapeutics*, *99*(3), 265–268.

Balta, S., Emirtekin, E., Kircaburun, K., & Griffiths, M. D. (2018). Neuroticism, trait fear of missing out, and phubbing: The mediating role of state fear of missing out and problematic Instagram use. *International Journal of Mental Health and Addiction*, 1–12.

Bandara, W., Miskon, S., & Fielt, E. (2011). A systematic, tool-supported method for conducting literature reviews in information systems. In *Proceedings of the 19th European Conference on Information Systems*, (pp. 1–14). AIS.

Bansal, G., Gefen, D., et al. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems*, *49*(2), 138–150.

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

Barrick, M. R. & Mount, M. K. (1991). The Big Five personality dimensions and job performance: A meta-analysis. *Personnel Psychology*, *44*(1), 1–26.

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.

Bartsch, M. & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior*, *56*, 147–154.

Basha, M. B., Mason, C., Shamsudin, M. F., Hussain, H. I., & Salem, M. A. (2015). Consumers attitude towards organic food. *Procedia Economics and Finance*, *31*, 444–452.

Bashir, M., Wee, C., Memon, N., & Guo, B. (2017). Profiling cybersecurity competition participants: Self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool. *Computers & Security*, *65*, 153–165.

Batorski, D. & Grzywińska, I. (2018). Three dimensions of the public sphere on Facebook. *Information, Communication & Society*, *21*(3), 356–374.

Baudrillard, J. (2016). *The consumer society: Myths and structures*. London, United Kingdom: Sage.

Bauer, S., Bernroider, E. W., & 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.

Bellman, S., Johnson, E. J., Kobrin, S. J., & Lohse, G. L. (2004). International differences in information privacy concerns: A global survey of consumers. *The Information Society*, *20*(5), 313–324.

Bennett, C. J. (1991). Computers, personal data, and theories of technology: Comparative approaches to privacy protection in the 1990s. *Science, Technology & Human Values*, *16*(1), 51–69.

Bennett, C. J. (2001). Cookies, web bugs, webcams and cue cats: Patterns of surveillance on the world wide web. *Ethics & Information Technology*, *3*(3), 195–208.

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 & People*, *28*(3), 426–441.

Benson, V., Saridakis, G., Tennakoon, H., & Ezingeard, 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*(1), 36–44.

Bercu, S. A. (1994). Toward universal surveillance in an information age economy: Can we handle treasury's new police technology? *Jurimetrics*, *34*(4), 383–449.

Bergström, A. (2015). Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses. *Computers in Human Behavior*, *53*(1), 419–426.

Birkin, M., Clarke, G., & Clarke, M. (2017). *Retail location planning in an era of multi-channel growth*. London, United Kingdom: Routledge.

Bland, J. M. & Altman, D. G. (1997). Statistics notes: Cronbach's alpha. *BMJ*, *314*(7080), 572.

Bloom, P. N., Milne, G. R., & Adler, R. (1994). Avoiding misuse of new information technologies: Legal and societal considerations. *The Journal of Marketing*, *58*(1), 98–110.

Blythe, J. M., Coventry, L., & Little, L. (2015). Unpacking security policy compliance: The motivators and barriers of employees' security behaviors. In *Proceedings of the 11th Symposium On Usable Privacy and Security*, (pp. 103–122). USENIX.

Bohner, G. & Wanke, M. (2002). *Attitudes and attitude change*. London, United Kingdom: Psychology Press.

Boo, Y.-K., Noh, J.-W., Kim, Y.-M., Kim, S.-S., & Rha, Y.-A. (2015). Perception of privacy and sensitivity of personal information among university students. *Culinary Science & Hospitality Research*, *21*(5), 25–37.

Boyd, D. M. & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, *13*(1), 210–230.

Boyes-Watson, C. (1994). Recordkeeping as a technology of power. *Berkeley Journal of Sociology*, *39*(1), 1–32.

Bozeman, B. & Bretschneider, S. (1986). Public management information systems: Theory and prescription. *Public Administration Review*, *46*(1), 475–487.

Brayne, S. (2017). Big data surveillance: The case of policing. *American Sociological Review*, *82*(5), 977–1008.

British Psychological Society (2007). Report of the working party on conducting research on the Internet: Guidelines for ethical practice in psychological research online. Retrieved from: https://goo.gl/PhvdVZ.

Briziarelli, M. & Flores, J. (2018). Mediation is the message: Social media ventures in informational capitalism. In S. Chhabra (Ed.), *Handbook of research on civic engagement and social change in contemporary society* (pp. 311–327). Hershey, United States of America: IGI Global.

Bronskill, J. (2019). 'Completely unacceptable': Canadian watchdog to take Facebook to court over privacy concerns. Retrieved from: https://globalnews.ca/news/5201868/facebook-canadians-privacy-watchdog/.

Brown, I. (2015). *Social media surveillance*. New York, United States of America: John Wiley & Sons.

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.

Burger, J. (2018). *Personality*. London, United Kingdom: Cengage Learning.

Burns, R. (2000). *Introduction to research methods*. London, United Kingdom: Sage.

Byrne, E. F. (1995). The two-tiered ethics of EDP. *Journal of Business Ethics*, *14*(1), 53–61.

Camadan, F., Reisoglu, I., Ursavas, Ö. F., & Mcilroy, D. (2018). How teachers' personality affect on their behavioral intention to use tablet PC. *The International Journal of Information and Learning Technology*, *35*(1), 12–28.

Carah, N. (2017). Algorithmic brands: A decade of brand experiments with mobile and social media. *New Media & Society*, *19*(3), 384–400.

Castañeda, J. A., Montoso, F. J., & Luque, T. (2007). The dimensionality of customer privacy concern on the Internet. *Online Information Review*, *31*(4), 420–439.

Cattell, R. B. (1966). The Scree Test for the number of factors. *Multivariate Behavioral Research*, *1*(2), 245–276.

Cecez-Kecmanovic, D. (2019). The resistible rise of the digital surveillance economy: A call for action. *Journal of Information Technology*, *34*(1), 81–83.

Cervone, D. & Pervin, L. (2014). *Personality Psychology*. New York, United States of America: John Wiley & Sons.

Chakraborty, R., Vishik, C., & Rao, H. R. (2013). Privacy preserving actions of older adults on social media: Exploring the behavior of opting out of information sharing. *Decision Support Systems*, *55*(4), 948–956.

Chamorro-Premuzic, T. (2016). *Personality and individual differences*. New York, United States of America: John Wiley & Sons.

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

Chang, C.-W. & Chen, G. M. (2014). College students' disclosure of location-related information on Facebook. *Computers in Human Behavior*, *35*, 33–38.

Chellappa, R. K. & Pavlou, P. A. (2002). Perceived information security, financial liability and consumer trust in electronic commerce transactions. *Logistics Information Management*, *15*(5/6), 358–368.

Chen, J. (2019). 15 Facebook stats every marketer should know for 2019. Retrieved from: https://sproutsocial.com/insights/facebook-stats-for-marketers.

Chen, R. & Sharma, S. K. (2015). Learning and self-disclosure behavior on social networking sites: the case of Facebook users. *European Journal of Information Systems*, *24*(1), 93–106.

Chen, R., Sharma, S. K., & Rao, H. R. (2016). Members' site use continuance on Facebook: Examining the role of relational capital. *Decision Support Systems*, *90*, 86–98.

Chen, T. (2011). Personality traits hierarchy of online shoppers. *International Journal of Marketing Studies*, *3*(4), 23.

Choi, B. C. & Land, L. (2016). The effects of general privacy concerns and transactional privacy concerns on Facebook apps usage. *Information & Management*, *53*(7), 868–877.

Cialdini, R. B., Reno, R. R., & Kallgren, C. A. (1990). A focus theory of normative conduct: Recycling the concept of norms to reduce littering in public places. *Journal of Personality and Social Psychology*, *58*(6), 1015.

Clarke, R. (1988). Information technology and dataveillance. *Communications of the ACM*, *31*(5), 498–512.

Clarke, R. (1994). The digital persona and its application to data surveillance. *The Information Society*, *10*(2), 77–92.

Clarke, R. (2001a). Person location and person tracking-technologies, risks and policy implications. *Information Technology & People*, *14*(2), 206–231.

Clarke, R. (2001b). While you were sleeping...surveillance technologies arrived. *AQ-East Melbourne*, *73*(1), 10–14.

Cobb-Clark, D. A. & Schurer, S. (2012). The stability of Big-Five personality traits. *Economics Letters*, *115*(1), 11–15.

Codish, D. & Ravid, G. (2014). Personality based gamification: How different personalities perceive gamification. In *Proceedings of the 22nd European Conference on Information Systems*, (pp. 1–12). AIS.

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences*. New York, United States of America: Lawrence Erlbaum Associates.

Coldewey, D. (2018). Facebook bans first app since Cambridge Analytica, myPersonality, and suspends hundreds more. Retrieved from: https://techcrunch.com/2018/08/22/facebook-bans-first-app-since-cambridge-analytica-mypersonality-and-suspends-hundreds-more/.

Conger, S., Pratt, J. H., & Loch, K. D. (2013). Personal information privacy and emerging technologies. *Information Systems Journal*, *23*(5), 401–417.

Correa, T., Hinsley, A. W., & De Zuniga, H. G. (2010). Who interacts on the web?: The intersection of users' personality and social media use. *Computers in Human Behavior*, *26*(2), 247–253.

Costa Jr, P. T. & McCrae, R. R. (1992). Four ways five factors are basic. *Personality and Individual Differences*, *13*(6), 653–665.

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

Cuganesan, S., Steele, C., & Hart, A. (2018). How senior management and workplace norms influence information security attitudes and self-efficacy. *Behaviour & Information Technology*, *37*(1), 50–65.

Culnan, M. J. (1993). "How did they get my name?": An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly*, *17*(3), 341–363.

Cusack, B. & Adedokun, K. (2018). The impact of personality traits on user's susceptibility to social engineering attacks. In *Proceedings of the 16th Australian Information Security Management Conference*, (pp. 83–89). ECU.

D'Arcy, J. & Lowry, P. B. (2019). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal*, *29*(1), 43–69.

Das, S., Kramer, A. D., Dabbish, L. A., & Hong, J. I. (2014). Increasing security sensitivity with social proof: A large-scale experimental confirmation. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, (pp. 739–749). ACM.

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.

Desai, K., Devulapalli, V., Agrawal, S., Kathiria, P., & Patel, A. (2017). Web crawler: Review of different types of web crawler, its issues, applications and research opportunities. *International Journal of Advanced Research in Computer Science*, *8*(3), 1199–1202.

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

Di Fabio, A., Palazzeschi, L., Bucci, O., Guazzini, A., Burgassi, C., & Pesce, E. (2018). Personality traits and positive resources of workers for sustainable development: Is emotional intelligence a mediator for optimism and hope? *Sustainability*, *10*(10), 3422.

Dickason, Z. & Ferreira, S. (2018). Establishing a link between risk tolerance, investor personality and behavioural finance in South Africa. *Cogent Economics & Finance*, *6*(1), 1–13.

DigitalWatch (2018). Cambridge Analytica explained: The facts, implications, and open questions. Retrieved from: https://dig.watch/trends/cambridge-analytica.

Dinev, T. & Hart, P. (2006). An extended Privacy Calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61–80.

Dodge, M. & Kitchin, R. (2005). Codes of life: Identification codes and the machine-readable world. *Environment and Planning D: Society and Space*, *23*(6), 851–881.

DOMO (2018). Data never sleeps 6.0. Retrieved from: https://www.domo.com/assets/downloads.

Dornan, P. & Hudson, J. (2003). Welfare governance in the surveillance society: A positive-realistic cybercriticalist view. *Social Policy & Administration*, *37*(5), 468–482.

Duffett, R. G. (2015). Facebook advertising's influence on intention-to-purchase and purchase amongst millennials. *Internet Research*, *25*(4), 498–526.

Eastin, M. S., Brinson, N. H., Doorey, A., & Wilcox, G. (2016). Living in a big data world: Predicting mobile commerce activity through privacy concerns. *Computers in Human Behavior*, *58*, 214–220.

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

Erevik, E. K., Pallesen, S., Andreassen, C. S., Vedaa, Ø., & Torsheim, T. (2018). Who is watching user-generated alcohol posts on social media? *Addictive Behaviors*, *78*, 131–137.

Esfandiar, K., Sharifi-Tehrani, M., Pratt, S., & Altinay, L. (2019). Understanding entrepreneurial intentions: A developed integrated structural model approach. *Journal of Business Research*, *94*, 172–182.

Eşkisu, M., Hoşoğlu, R., & Rasmussen, K. (2017). An investigation of the relationship between Facebook usage, Big Five, self-esteem and Narcissism. *Computers in Human Behavior*, *69*, 294–301.

Farnden, J., Martini, B., & Choo, K.-K. R. (2015). Privacy risks in mobile dating apps. In *Proccedings of the 21st Americas Conference on Information Systems*, (pp. 1–16). AIS.

Fatima, R., Yasin, A., Liu, L., Wang, J., Afzal, W., & Yasin, A. (2019). Sharing information online rationally: An observation of user privacy concerns and awareness using serious game. *Journal of Information Security and Applications*, *48*, 1–16.

Fayn, K., Tiliopoulos, N., & MacCann, C. (2015). Interest in truth versus beauty: Intellect and Openness reflect different pathways towards interest. *Personality and Individual Differences*, *81*, 47–52.

Fink, G. A., Zarzhitsky, D. V., Carroll, T. E., & Farquhar, E. D. (2015). Security and privacy grand challenges for the Internet of Things. In *2015 International Conference on Collaboration Technologies and Systems*, (pp. 27–34). IEEE.

Fishbein, M. & Yzer, M. C. (2003). Using theory to design effective health behavior interventions. *Communication Theory*, *13*(2), 164–183.

Flores, W. R. & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security*, *59*, 26–44.

Formanek, T. & Tahal, R. (2018). Analysis of personal data-sharing consent factors, with focus on loyalty programs in the Czech Republic. *Business: Theory and Practice*, *19*, 70.

Fornara, F., Pattitoni, P., Mura, M., & Strazzera, E. (2016). Predicting intention to improve household energy efficiency: The role of value-belief-norm theory, normative and informational influence, and specific attitude. *Journal of Environmental Psychology*, *45*, 1–10.

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

Frackman, A., Martin, R. C., & Ray, C. (2002). *Internet and online privacy: A legal and business guide*. New York, United States of America: ALM Publishing.

Freitag, M. & Bauer, P. C. (2016). Personality traits and the propensity to trust friends and strangers. *The Social Science Journal*, *53*(4), 467–476.

Fricker, R. D. (2008). *Sampling methods for web and e-mail surveys.* Sage Publications New Delhi, India.

Fuchs, C. (2011). An alternative view of privacy on Facebook. *Information*, *2*(1), 140–165.

Fuchs, C. (2015). *Reading Marx in the information age: A media and communication studies perspective on capital volume 1.* London, United Kingdom: Routledge.

Fuchs, C. (2017). *Social media: A critical introduction.* London, United Kingdom: Sage.

Fuchs, C. & Trottier, D. (2015). Towards a theoretical model of social media surveillance in contemporary society. *Communications*, *40*(1), 113–135.

Fukuta, Y., Murata, K., Adams, A. A., Orito, Y., & Palma, A. M. L. (2017). Personal data sensitivity in Japan. *ORBIT Journal*, *1*(2), 1–13.

Gefen, D. & Straub, D. (2005). A practical guide to factorial validity using PLS-Graph: Tutorial and annotated example. *Communications of the Association for Information Systems*, *16*(1), 91–109.

Gefen, D., Straub, D., & Boudreau, M.-C. (2000). Structural equation modeling and regression: Guidelines for research practice. *Communications of the Association for Information Systems*, *4*(1), 2–76.

Geisser, S. & Eddy, W. F. (1979). A predictive approach to model selection. *Journal of the American Statistical Association*, *74*(365), 153–160.

Giles, D. (2013). *Advanced research methods in Psychology.* London, United Kingdom: Routledge.

Giluk, T. L. & Postlethwaite, B. E. (2015). Big Five personality and academic dishonesty: A meta-analytic review. *Personality and Individual Differences*, *72*, 59–67.

Giroux, H. A. (2015). Totalitarian paranoia in the post-Orwellian surveillance state. *Cultural Studies*, *29*(2), 108–140.

Godlove, T. (2012). Examination of the factors that influence teleworkers' willingness to comply with information security guidelines. *Information Security Journal: A Global Perspective*, *21*(4), 216–229.

Gohary, A. & Hanzaee, 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.

Golbeck, J. & Mauriello, M. (2016). User perception of Facebook app data access: A comparison of methods and privacy concerns. *Future Internet*, *8*(2), 1–14.

Goodboy, A. K. & Martin, M. M. (2015). The personality profile of a cyberbully: Examining the Dark Triad. *Computers in Human Behavior*, *49*, 1–4.

Gordon, M. & Ortutay, B. (2019). Facebook to pay 5 billion dollars for privacy mishaps in largest FTC penalty on tech company. Retrieved from: https://globalnews.ca/news/5676260/facebook-fined-5-billion-privacy-violations/.

Gosling, S. D., Rentfrow, P. J., & Swann Jr, W. B. (2003). A very brief measure of the Big Five personality domains. *Journal of Research in Personality*, *37*(6), 504–528.

Goss, J. (1995). "We know who you are and we know where you live": The instrumental rationality of geodemographic systems. *Economic Geography*, *71*(2), 171–198.

Gotterbarn, D. (1999). Privacy lost: The Net, autonomous agents, and 'virtual information'. *Ethics and Information Technology*, *1*(2), 147–154.

Gotterbarn, D. (2016). The creation of facts in the cloud: A fiction in the making. *ACM SIGCAS Computers and Society*, *45*(3), 60–67.

Graham, J. (2019). Despite controversies, Facebook apps were the most used and downloaded in 2018. Retrieved from: https://www.usatoday.com/story/tech/talkingtech/2019/01/16/despite-privacy-concerns-facebook-apps-most-used-2018/2573650002/.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security*, *73*, 345–358.

Gray, S. H. (1989). Electronic databases and privacy: Policy for the 1990s. *Science, Technology, & Human Values*, *14*(3), 242–257.

Greenwald, G. & Ackerman, S. (2013). NSA collected US email records in bulk for more than two years under Obama. Retrieved from: https://goo.gl/4TDnoH.

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.

Gudivada, V. N., Baeza-Yates, R., & Raghavan, V. V. (2015). Big data: Promises and problems. *Computer*, (3), 20–23.

Haeussinger, F. & Kranz, J. (2013). Information security awareness: Its antecedents and mediating effects on security compliant behavior. In *Proccedings of the 34th International Conference on Information Systems*, (pp. 1–16). AIS.

Hair, J., Black, W., Babin, B., & Anderson, R. (2013). *Multivariate data analysis* (7 ed.). Pearson Higher Education.

Hair, J., Hult, G., Ringle, C., & Sarstedt, M. (2017). *A primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. Los Angeles, United States of America: Sage publications.

Hajian, S., Bonchi, F., & Castillo, C. (2016). Algorithmic bias: From discrimination discovery to fairness-aware data mining. In *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, (pp. 2125–2126). ACM.

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

Hallam, C. & Zanella, G. (2017). Online self-disclosure: The Privacy Paradox explained as a temporally discounted balance between concerns and rewards. *Computers in Human Behavior*, *68*, 217–227.

Ham, M., Jeger, M., & Frajman Ivković, A. (2015). The role of subjective norms in forming the intention to purchase green food. *Economic Research*, *28*(1), 738–748.

Hamati-Ataya, I. (2012). Beyond Post-Positivism: The missed promises of systemic pragmatism. *International Studies Quarterly*, *56*(2), 291–305.

Hansla, A., Gamble, A., Juliusson, A., & Gärling, T. (2008). The relationships between awareness of consequences, environmental concern, and value orientations. *Journal of Environmental Psychology*, *28*(1), 1–9.

Hanus, B. & Wu, Y. A. (2016). Impact of users' security awareness on desktop security behavior: A Protection Motivation Theory perspective. *Information Systems Management*, *33*(1), 2–16.

Hao, Q., Yang, W., & Shi, Y. (2019). Characterizing the relationship between conscientiousness and knowledge sharing behavior in virtual teams: An interactionist approach. *Computers in Human Behavior*, *91*, 42–51.

Hargittai, E. & Marwick, A. (2016). "What can i really do?" explaining the Privacy Paradox with online apathy. *International Journal of Communication*, *10*, 3737–3757.

Harkin, D., Molnar, A., & Vowles, E. (2019). The commodification of mobile phone surveillance: An analysis of the consumer spyware industry. *Crime, Media, Culture*.

Hayden, M. (2014). State surveillance. Retrieved from: https://goo.gl/WD7M7M.

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.

Hazari, S., Hargrave, W., & Clenney, B. (2008). An empirical investigation of factors influencing information security behavior. *Journal of Information Privacy and Security*, *4*(4), 3–20.

Heinze, N. & Hu, Q. (2007). Why college undergraduates choose to major in information technology: A multi-theoretical perspective. In *Proceedings of the 13th Americas Conference on Information Systems*, (pp. 249–258). AIS.

Herath, T. & Rao, H. R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154–165.

Herath, T. & Rao, H. R. (2009b). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125.

Heyman, R., De Wolf, R., & Pierson, J. (2014). Evaluating social media privacy settings for personal and advertising purposes. *Info*, *16*(4), 18–32.

Hilton, J. L., Fein, S., & Miller, D. T. (1993). Suspicion and dispositional inference. *Personality and Social Psychology Bulletin*, *19*(5), 501–512.

Hirschprung, R., Toch, E., Bolton, F., & Maimon, O. (2016). A methodology for estimating the value of privacy in information disclosure systems. *Computers in Human Behavior*, *61*, 443–453.

Hitlin, P. & Rainie, L. (2019). Facebook algorithms and personal data. Retrieved from: https://www.pewinternet.org/2019/01/16/facebook-algorithms-and-personal-data/.

Hollenbaugh, E. E. & Ferris, A. L. (2014). Facebook self-disclosure: Examining the role of traits, social cohesion, and motives. *Computers in Human Behavior*, *30*, 50–58.

Hughes, D. J., Rowe, M., Batey, M., & Lee, A. (2012). A tale of two sites: Twitter vs. Facebook and the personality predictors of social media usage. *Computers in Human Behavior*, *28*(2), 561–569.

Humaidi, N. & Balakrishnan, V. (2015). Leadership styles and information security compliance behavior: The mediator effect of information security awareness. *International Journal of Information and Education Technology*, *5*(4), 311.

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, *51*(1), 69–79.

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.

Jai, T.-M. C. & King, N. J. (2016). Privacy versus reward: Do loyalty programs increase consumers' willingness to share personal information with third-party advertisers and data brokers? *Journal of Retailing and Consumer Services*, *28*, 296–303.

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.

Jayaram, D., Manrai, A. K., & Manrai, L. A. (2015). Effective use of marketing technology in Eastern Europe: Web analytics, social media, customer analytics, digital campaigns and mobile applications. *Journal of Economics, Finance and Administrative Science*, *20*(39), 118–132.

Jayawardhena, C. (2004). Personal values' influence on e-shopping attitude and behaviour. *Internet Research*, *14*(2), 127–138.

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.

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.

John, O. P. & Srivastava, S. (1999). The Big Five trait taxonomy: History, measurement, and theoretical perspectives. *Handbook of Personality: Theory and Research*, *2*(1999), 102–138.

Johnston, A. C. & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, *34*(3), 549–566.

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.

Jordaan, Y. & Van Heerden, G. (2017). Online privacy-related predictors of Facebook usage intensity. *Computers in Human Behavior*, *70*, 90–96.

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.

Junglas, I. & Spitzmuller, C. (2006). Personality traits and privacy perceptions: An empirical study in the context of location-based services. In *2006 International Conference on Mobile Business*, (pp. 36–36). IEEE.

Kaiser, H. F. (1974). An index of factorial simplicity. *Psychometrika*, *39*(1), 31–36.

Kamleitner, B. & Mitchell, V. (2019). Your data is my data: A framework for addressing interdependent privacy infringements. *Journal of Public Policy & Marketing*, *38*(4), 433–450.

Kang, J. (1998). Information privacy in cyberspace transactions. *Stanford Law Review*, *50*(4), 1193–1294.

Kaplan, A. M. & Haenlein, M. (2010). Users of the world, unite! the challenges and opportunities of social media. *Business Horizons*, *53*(1), 59–68.

Kardum, I., Hudek-knezevic, J., Schmitt, D. P., & Covic, M. (2017). Assortative mating for Dark Triad: Evidence of positive, initial, and active assortment. *Personal Relationships*, *24*(1), 75–83.

Karim, N. S. A., Zamzuri, N. H. A., & Nor, Y. M. (2009). Exploring the relationship between Internet ethics in university students and the Big Five model of personality. *Computers & Education*, *53*(1), 86–93.

Karimi, S., Biemans, H. J., Naderi Mahdei, K., Lans, T., Chizari, M., & Mulder, M. (2017). Testing the relationship between personality characteristics, contextual factors and entrepreneurial intentions in a developing country. *International Journal of Psychology*, *52*(3), 227–240.

Karwatzki, S., Dytynko, O., Trenz, M., & Veit, D. (2017). Beyond the personalization-Privacy Paradox: Privacy valuation, transparency features, and service personalization. *Journal of Management Information Systems*, *34*(2), 369–400.

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the Privacy Calculus. *Information Systems Journal*, *25*(6), 607–635.

Keiber, J. (2015). Surveillance hegemony. *Surveillance & Society*, *13*(2), 168–181.

Kelloway, E. K. (1995). Structural Equation Modelling in perspective. *Journal of Organizational Behavior*, *16*(3), 215–224.

Kelly, E. V., Newton, N. C., Stapinski, L. A., & Teesson, M. (2018). Prospective associations between personality and bullying among Australian adolescents. *Australian & New Zealand Journal of Psychiatry*, *52*(2), 173–180.

Kelman, H. C. (1958). Compliance, identification, and internalization three processes of attitude change. *Journal of Conflict Resolution*, *2*(1), 51–60.

Kezer, M., Sevi, B., Cemalcilar, Z., & Baruh, L. (2016). Age differences in privacy attitudes, literacy and privacy management on Facebook. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *10*(1), 1–20.

Ki-Aries, D. & Faily, S. (2017). Persona-centred information security awareness. *Computers & Security*, *70*, 663–674.

Kim, J. W. & Chock, T. M. (2017). Personality traits and psychological motivations predicting selfie posting behaviors on social networking sites. *Telematics and Informatics*, *34*(5), 560–571.

Kim, M.-S. & Hunter, J. E. (1993). Relationships among attitudes, behavioral intentions, and behavior: A meta-analysis of past research. *Communication Research*, *20*(3), 331–364.

Kircaburun, K., Demetrovics, Z., & Tosuntaş, Ş. B. (2018). Analyzing the links between problematic social media use, Dark Triad traits, and self-esteem. *International Journal of Mental Health and Addiction*, 1–12.

Kisyovska, Y., Krönung, J., & Eckhardt, A. (2015). Peer influence, family dysfunction or conditioning?-an empirical analysis of Facebook addiction predispositions. In *Proceedings of the 12th International Conference on Wirtschaftsinformatik*, (pp. 1874–1889). AIS.

Kling, R., Ackerman, M. S., & Allen, J. P. (1995). Information entrepreneurialism, information technologies, and the continuing vulnerability of privacy. In *Computerization and Controversy (2nd ed.)*, (pp. 727–743). Academic Press, Inc.

Knigge, L. & Cope, M. (2006). Grounded visualization: Integrating the analysis of qualitative and quantitative data through grounded theory and visualization. *Environment and Planning*, *38*(11), 2021–2037.

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.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the Privacy Paradox phenomenon. *Computers & Security*, *64*, 122–134.

Komarraju, M., Karau, S. J., Schmeck, R. R., & Avdic, A. (2011). The Big Five personality traits, learning styles, and academic achievement. *Personality and Individual Differences*, *51*(4), 472–477.

König, M. C. (2016). Transnational border surveillance and social sorting systems in the EU: A changing approach to Europe's borders? *MaRBLe*, *3*, 1–25.

Koohikamali, M., Peak, D. A., & Prybutok, V. R. (2017). Beyond self-disclosure: Disclosure of information about others in social network sites. *Computers in Human Behavior*, *69*, 29–42.

Korff, D., Wagner, B., Powles, J., Avila, R., & Buermeyer, U. (2017). Boundaries of law: Exploring transparency, accountability, and oversight of government surveillance regimes. *SSRN*, *2017*(16), 1–72.

Kosinski, M., Matz, S. C., Gosling, S. D., Popov, V., & Stillwell, D. (2015). Facebook as a research tool for the social sciences: Opportunities, challenges, ethical considerations, and practical guidelines. *American Psychologist*, *70*(6), 543–556.

Kothari, C. R. (2004). *Research methodology: Methods and techniques*. New Delhi, India: New Age International.

Krasnova, H., Günther, O., Spiekermann, S., & Koroleva, K. (2009). Privacy concerns and identity in online social networks. *Identity in the Information Society*, *2*(1), 39–63.

Kuem, J., Ray, S., Siponen, M., & Kim, S. S. (2017). What leads to prosocial behaviors on social networking services: A tripartite model. *Journal of Management Information Systems*, *34*(1), 40–70.

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.

Kypri, K. & Gallagher, S. J. (2003). Incentives to increase participation in an Internet survey of alcohol use: A controlled experiment. *Alcohol and Alcoholism*, *38*(5), 437–441.

Lam, E. T. H., Au, C. H., & Chiu, D. K. (2019). Analyzing the use of Facebook among university libraries in Hong Kong. *The Journal of Academic Librarianship*, *45*(3), 175–183.

Lambert, C. E., Arbuckle, S. A., & Holden, R. R. (2016). The Marlowe–Crowne social desirability scale outperforms the BIDR impression management scale for identifying fakers. *Journal of Research in Personality*, *61*, 80–86.

Lane, W. & Manner, C. (2011). The impact of personality traits on smartphone ownership and use. *International Journal of Business and Social Science*, *2*(17), 22–28.

Lanier, M. M. & Cooper, A. T. (2016). From papyrus to cyber: How technology has directed law enforcement policy and practice. *Criminal Justice Studies*, *29*(2), 92–104.

Lapinski, M. K. & Rimal, R. N. (2005). An explication of social norms. *Communication Theory*, *15*(2), 127–147.

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.

Lee, Y. & Kozar, K. A. (2005). Investigating factors affecting the adoption of anti-spyware systems. *Communications of the ACM*, *48*(8), 72–77.

Leetaru, K. (2018). Facebook's device partners and how nothing has changed since Cambridge Analytica. Retrieved from: https://www.forbes.com/sites/kalevleetaru/2018/06/18/facebooks-device-partners-and-how-nothing-has-changed-since-cambridge-analytica.

Leutner, F., Ahmetoglu, G., Akhtar, R., & Chamorro-Premuzic, T. (2014). The relationship between the entrepreneurial personality and the Big Five personality traits. *Personality and Individual Differences*, *63*, 58–63.

Li, K., Lin, Z., & Wang, X. (2015). An empirical analysis of users' privacy disclosure behaviors on social network sites. *Information & Management*, *52*(7), 882–891.

Lichy, J., Kachour, M., & Khvatova, T. (2017). Big data is watching YOU: Opportunities and challenges from the perspective of young adult consumers in Russia. *Journal of Marketing Management*, *33*(9-10), 719–741.

Lima, A. C. E. & De Castro, L. N. (2014). A multi-label, semi-supervised classification approach applied to personality prediction in social media. *Neural Networks*, *58*, 122–130.

Liu, Y. & Fan, J. (2015). Culturally specific privacy practices on social network sites: Privacy boundary permeability management in photo sharing by American and Chinese college-age users. *International Journal of Communication*, *9*, 2141–2060.

Lodder, A. R. & Loui, R. (2018). Research handbook of law and artificial intelligence. In W. Barfield & U. Pagallo (Eds.), *Data algorithms and privacy in surveillance: On stages, numbers and the human factor* (pp. 1–11). London, United Kingdom: SSRN.

Lönnqvist, J.-E. & Itkonen, J. V. (2016). Homogeneity of personal values and personality traits in Facebook social networks. *Journal of Research in Personality*, *60*, 24–35.

Lorica, B. (2008). Facebook app categories ranked by usage. Retrieved from: http://radar.oreilly.com/2008/05/facebook-app-categories.html.

Lowry, P. B., Cao, J., & Everard, A. (2011). Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. *Journal of Management Information Systems*, *27*(4), 163–200.

Lowry, P. B., D'Arcy, J., Hammer, B., & Moody, G. D. (2016). "Cargo Cult" science in traditional organization and information systems survey research: A case for using nontraditional methods of data collection, including Mechanical Turk and online panels. *The Journal of Strategic Information Systems*, *25*(3), 232–240.

Lupton, D. (2012). M-health and health promotion: The digital cyborg and surveillance society. *Social Theory & Health*, *10*(3), 229–244.

Lutz, C., Hoffmann, C. P., Bucher, E., & Fieseler, C. (2018). The role of privacy concerns in the sharing economy. *Information, Communication & Society*, *21*(10), 1472–1492.

Lyon, D. (1992). The new surveillance: Electronic technologies and the maximum security society. *Crime, Law & Social Change*, *18*(1), 159–175.

Lyon, D. (2001). Facing the future: Seeking ethics for everyday surveillance. *Ethics & Information Technology*, *3*(3), 171–180.

Lyon, D. (2016). Surveillance, liquidity and the ethics of visibility. *Revue Internationale de Philosophie*, (3), 365–379.

Mackenzie, N. & Knipe, S. (2006). Research dilemmas: Paradigms, methods and methodology. *Issues in Educational Research*, *16*(2), 193–205.

Malcolm, J. P. (2013). *Financial globalization and the opening of the Japanese economy*. London, United Kingdom: Routledge.

Mamonov, S. & Benbunan-Fich, R. (2017). Exploring factors affecting social e-commerce service adoption: The case of Facebook gifts. *International Journal of Information Management*, *37*(6), 590–600.

Mamonov, S. & Benbunan-Fich, R. (2018). The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior*, *83*, 32–44.

Marichal, J. (2016). *Facebook democracy (open access): The architecture of disclosure and the threat to public life*. London, United Kingdom: Routledge.

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.

Martinez, R. (2017). *Creating freedom: The lottery of birth, the lllusion of consent, and the fight for our future*. Edinburgh, Scotland: Canongate Books.

Marwick, A. (2012). The public domain: Surveillance in everyday life. *Surveillance & Society*, *9*(4), 378–393.

Marx, G. (2001). Technology and social control: The search for the illusive silver bullet. Retrieved from: https://goo.gl/uQGkYS.

Mascarenhas, O. A. (1995). Exonerating unethical marketing executive behaviors: A diagnostic framework. *The Journal of Marketing*, *59*(2), 43–57.

Maulana, I. (2019). Big brothers are seducing you: Consumerism, surveillance, and the agency of consumers. In O. Ozgen (Ed.), *Handbook of research on consumption, media, and popular culture in the global age* (pp. 57–75). Hershey, United States of America: IGI Global.

Mayer, J., Mutchler, P., & Mitchell, J. C. (2016). Evaluating the privacy properties of telephone metadata. *Proceedings of the National Academy of Sciences*, *113*(20), 5536–5541.

McCormac, A., Calic, D., Butavicius, M., Parsons, K., Zwaans, T., & Pattinson, M. (2017). A reliable measure of information security awareness and the identification of bias in responses. *Australasian Journal of Information Systems*, *21*, 1–12.

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.

McCrohan, K. F. (1989). Information technology, privacy, and the public good. *Journal of Public Policy & Marketing*, *8*(1), 265–278.

Merhi, M. I. & Ahluwalia, P. (2019). Examining the impact of deterrence factors and norms on resistance to information systems security. *Computers in Human Behavior*, *92*, 37–46.

Mertens, D. M. (2014). *Research and evaluation in education and psychology: Integrating diversity with quantitative, qualitative, and mixed methods*. Los Angeles, United States of America: Sage.

Miller, K. (2000). Common ground from the Post-Positivist perspective. In S. Corman & M. Poole (Eds.), *Perspectives on organizational communication: Finding common ground* (pp. 46–67). New York, United States of America: The Guilford Press.

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.

Minton, E. A., Spielmann, N., Kahle, L. R., & Kim, C.-H. (2018). The subjective norms of sustainable consumption: A cross-cultural exploration. *Journal of Business Research*, *82*, 400–408.

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.

Moreira, A. C., Fortes, N., & Santiago, R. (2017). Influence of sensory stimuli on brand experience, brand equity and purchase intention. *Journal of Business Economics and Management*, *18*(1), 68–83.

Moro, S., Cortez, P., & Rita, P. (2014). A data-driven approach to predict the success of bank telemarketing. *Decision Support Systems*, *62*, 22–31.

Moro, S., Rita, P., & Vala, B. (2016). Predicting social media performance metrics and evaluation of the impact on brand building: A data mining approach. *Journal of Business Research*, *69*(9), 3341–3351.

Morris, M. W. & Liu, Z. (2015). Psychological functions of subjective norms: Reference groups, moralization, adherence, and defiance. *Journal of Cross-Cultural Psychology*, *46*(10), 1279–1287.

Murphy, P. E. (2015). *Ethics of marketing*. New York, United States of America: Wiley.

Murray, D. & Fussey, P. (2019). Bulk surveillance in the digital age: Rethinking the human rights law approach to bulk monitoring of communications data. *Israel Law Review*, *52*(1), 31–60.

Myers, M. D. & Klein, H. K. (2011). A set of principles for conducting critical research in information systems. *MIS Quarterly*, *35*(1), 17–36.

Nam, T. (2017). Does ideology matter for surveillance concerns? *Telematics and Informatics*, *34*(8), 1572–1585.

Neves, J., Narducci, F., Barra, S., & Proença, H. (2016). Biometric recognition in surveillance scenarios: A survey. *Artificial Intelligence Review*, *46*(4), 515–541.

Nguyen, T. N., Lobo, A., & Greenland, S. (2016). Pro-environmental purchase behaviour: The role of consumers' biospheric values. *Journal of Retailing and Consumer Services*, *33*, 98–108.

Ngwenyama, O. K. (1991). The critical social theory approach to information systems: Problems and challenges. In H. Nissen, H. Klein, & R. Hirschheim (Eds.), *Information systems research: Contemporary approaches and emergent traditions* (pp. 267–280). Amsterdam, Holland: North-Holland.

Nissenbaum, H. (2018). Respecting context to protect privacy: Why meaning matters. *Science and Engineering Ethics*, *24*(3), 831–852.

O'Brien, D. G. & Yasnoff, W. A. (1999). Privacy, confidentiality, and security in information systems of state health agencies. *American Journal of Preventive Medicine*, *16*(4), 351–358.

O'Dwyer, R. (2019). Cache society: Transactional records, electronic money, and cultural resistance. *Journal of Cultural Economy*, *12*(2), 133–153.

O'Leary, Z. (2004). *The essential guide to doing research*. Los Angeles, United States of America: Sage.

Ong, E. Y., Ang, R. P., Ho, J. C., Lim, J. C., Goh, D. H., Lee, C. S., & Chua, A. Y. (2011). Narcissism, Extraversion and adolescents' self-presentation on Facebook. *Personality and Individual Differences*, *50*(2), 180–185.

Orlikowski, W. J. & Baroudi, J. J. (1991). Studying information technology in organizations: Research approaches and assumptions. *Information Systems Research*, *2*(1), 1–28.

Ortigosa, A., Carro, R. M., & Quiroga, J. I. (2014). Predicting user personality by mining social interactions in Facebook. *Journal of Computer and System Sciences*, *80*(1), 57–71.

Ortiz, J., Chih, W.-H., & Tsai, F.-S. (2018). Information privacy, consumer alienation, and lurking behavior in social networking sites. *Computers in Human Behavior*, *80*, 143–157.

Osatuyi, B. (2015). Personality traits and information privacy concern on social media platforms. *Journal of Computer Information Systems*, *55*(4), 11–19.

Padyab, A., Päivärinta, T., Ståhlbröst, A., & Bergvall-Kåreborn, B. (2019). Awareness of indirect information disclosure on social network sites. *Social Media+ Society*, *5*(2), 1–14.

Palmer, D. E. (2005). Pop-ups, cookies, and spam: Toward a deeper analysis of the ethical significance of Internet marketing practices. *Journal of Business Ethics*, *58*(1-3), 271–280.

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.

Parkinson, B., Millard, D. E., O'Hara, K., & Giordano, R. (2018). The digitally extended self: A lexicological analysis of personal data. *Journal of Information Science*, *44*(4), 552–565.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. *Computers & Security*, *66*, 40–51.

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., & Calic, D. (2017). Managing information security awareness at an Australian bank: A comparative study. *Information & Computer Security*, *25*(2), 181–189.

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.

Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS Quarterly*, *31*(1), 105–136.

Pavone, V., Ball, K., Degli Esposti, S., Dibb, S., & Santiago-Gómez, E. (2018). Beyond the security paradox: Ten criteria for a socially informed security policy. *Public Understanding of Science*, *27*(6), 638–654.

Pegg, D. & Cadwalladr, C. (2018). Us data firm admits employee approached Cambridge Analytica: Palantir confirm employee engaged in a personal capacity with the company. Retrieved from: https://www.theguardian.com/uk-news/2018/mar/28/palantir-employee-cambridge-analytica.

Peleg, S., Vilchinsky, N., Fisher, W. A., Khaskia, A., & Mosseri, M. (2017). Personality makes a difference: Attachment orientation moderates Theory of Planned Behavior prediction of cardiac medication adherence. *Journal of Personality*, *85*(6), 867–879.

Pentina, I., Zhang, L., & Basmanova, O. (2013). Antecedents and consequences of trust in a social media brand: A cross-cultural study of Twitter. *Computers in Human Behavior*, *29*(4), 1546–1555.

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.

Perinelli, E. & Gremigni, P. (2016). Use of social desirability scales in clinical psychology: A systematic review. *Journal of Clinical Psychology*, *72*(6), 534–551.

Perrin, A. & Anderson, M. (2019). Share of U.S. adults using social media, including Facebook, is mostly unchanged since 2018. Reteived from: https://www.pewresearch.org/fact-tank/2019/04/10/share-of-u-s-adults-using-social-media-including-facebook-is-mostly-unchanged-since-2018/.

Perugini, M. & Bagozzi, R. P. (2001). The role of desires and anticipated emotions in goal-directed behaviours: Broadening and deepening the Theory of Planned Behaviour. *British Journal of Social Psychology*, *40*(1), 79–98.

Pervin, L. A. & John, O. P. (1997). *Personality: Theory and research.* New York, United States of America: John Wiley & Sons.

Peters, M. D., Godfrey, C. M., Khalil, H., McInerney, P., Parker, D., & Soares, C. B. (2015). Guidance for conducting systematic scoping reviews. *International Journal of Evidence-based Healthcare*, *13*(3), 141–146.

Petter, S., Straub, D. W., & Rai, A. (2007). Specifying formative constructs in Information Systems research. *MIS Quaterly*, *31*(4), 657–679.

Pew Research Center (2019a). 10 facts about Americans and Facebook. Retrieved from: https://www.pewresearch.org/fact-tank/2019/05/16/facts-about-americans-and-facebook/.

Pew Research Center (2019b). Social media fact sheet. Retrieved from: https://www.pewinternet.org/fact-sheet/social-media/.

Pincus, L. B. & Johns Jr, R. J. (1997). Private parts: A global analysis of privacy protection schemes and a proposed innovation for their comparative evaluation. In M. Fleckenstein, M. Maury, L. Pincus, & P. Primeaux (Eds.), *From the universities to the marketplace: The business ethics journey* (pp. 27–50). London, United Kingdom: Springer.

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, *88*(5), 879.

Posey, C., Lowry, P. B., Roberts, T. L., & Ellis, T. S. (2010). Proposing the online community self-disclosure model: The case of working professionals in France and the UK who use online communities. *European Journal of Information Systems*, *19*(2), 181–195.

Pu, Y. & Grossklags, J. (2015). Using conjoint analysis to investigate the value of interdependent privacy in social app adoption scenarios. In *Proceedings of the 36th International Conference on Information Systems*, (pp. 1–20). AIS.

Punch, K. (2003). *Survey research: The basics*. Los Angeles: United States of America: Sage.

Qiu, L., Lin, H., Ramsay, J., & Yang, F. (2012). You are what you tweet: Personality expression and perception on Twitter. *Journal of Research in Personality*, *46*(6), 710–718.

Rahman, H. U., Rehman, A. U., Nazir, S., Rehman, I. U., & Uddin, N. (2019). Advances in information and communication. In A. K. & B. R. (Eds.), *Privacy and security—limits of personal information to minimize loss of privacy*, volume 70 (pp. 964–974). London, United Kingdom: Springer.

Rajamäki, J., Tervahartiala, J., Tervola, S., Johansson, S., Ovaska, L., & Rathod, P. (2012). How transparency improves the control of law enforcement authorities' activities? In *2012 European Intelligence and Security Informatics Conference*, (pp. 14–21). IEEE.

Rao, P. R. M., Krishna, S. M., & Kumar, A. S. (2018). Privacy preservation techniques in big data analytics: A survey. *Journal of Big Data*, *5*(33), 1–12.

Ray, J. J. (1984). The reliability of short social desirability scales. *The Journal of Social Psychology*, *123*(1), 133–134.

Raykov, T. (1997). Estimation of composite reliability for congeneric measures. *Applied Psychological Measurement*, *21*(2), 173–184.

Reeve, A. (2019). Exercising control at the urban scale: Towards a theory of spatial organisation and surveillance. In A. Flynn & A. Mackay (Eds.), *Surveillance, architecture and control* (pp. 19–56). London, United Kingdom: Springer.

Rhodes, R. E. & Courneya, K. S. (2003). Investigating multiple components of attitude, subjective norm, and perceived control: An examination of the Theory of Planned Behaviour in the exercise domain. *British Journal of Social Psychology*, *42*(1), 129–146.

Riquelme, I. P. & Román, S. (2014). Is the influence of privacy and security on online trust the same for all type of consumers? *Electronic Markets*, *24*(2), 135–149.

Ritzer, G. & Jurgenson, N. (2010). Production, consumption, prosumption: The nature of capitalism in the age of the digital 'prosumer'. *Journal of Consumer Culture*, *10*(1), 13–36.

Robbin, A. (2001). The loss of personal privacy and its consequences for social research. *Journal of Government Information*, *28*(5), 493–527.

Rogers, M. & Eden, G. (2017). The Snowden disclosures, technical standards and the making of surveillance infrastructures. *International Journal of Communication*, *11*, 802–823.

Rosamond, E. (2015). Technologies of attribution: Characterizing the citizen-consumer in surveillance performance. *International Journal of Performance Arts and Digital Media*, *11*(2), 148–164.

Ross, C., Orr, E. S., Sisic, M., Arseneault, J. M., Simmering, M. G., & Orr, R. R. (2009). Personality and motivations associated with Facebook use. *Computers in Human Behavior*, *25*(2), 578–586.

Ruckenstein, M. & Granroth, J. (2019). Algorithms, advertising and the intimacy of surveillance. *Journal of Cultural Economy*, 1–14.

Rule, J. B., McAdam, D., Stearns, L., & Uglow, D. (1983). Documentary identification and mass surveillance in the United States. *Social Problems*, *31*(2), 222–234.

Ryan, A. B. (2006). Post-Positivist approaches to research. *Researching and writing your thesis: A guide for postgraduate students*, 12–26.

Ryan, T. & Xenos, S. (2011). Who uses Facebook? an investigation into the relationship between the Big Five, shyness, Narcissism, loneliness, and Facebook usage. *Computers in Human Behavior*, *27*(5), 1658–1664.

Safa, N. S., Maple, C., Watson, T., & Furnell, S. (2017). Information security collaboration formation in organisations. *IET Information Security*, *12*(3), 238–245.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*, 65–78.

Safa, N. S. & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior*, *57*, 442–451.

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, *56*, 70–82.

Sakaki, T., Okazaki, M., & Matsuo, Y. (2010). Earthquake shakes Twitter users: Real-time event detection by social sensors. In *Proceedings of the 19th International Conference on World Wide Web*, (pp. 851–860). ACM.

Salloum, S. A., Al-Emran, M., Monem, A. A., & Shaalan, K. (2017). A survey of text mining in social media: Facebook and Twitter perspectives. *Advances in Science, Technology and Engineering Systems Journal*, *2*(1), 127–133.

Saridakis, G., Benson, V., Ezingeard, J.-N., & Tennakoon, H. (2016). Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. *Technological Forecasting and Social Change*, *102*, 320–330.

Saunders, M., Lewis, P., & Thornhill, A. (2016). *Research methods for business students* (7th ed.). London, United Kingdom: Pearson.

Schaarschmidt, M., Ivens, S., Homscheid, D., & Bilo, P. (2015). Crowdsourcing for survey research: Where Amazon Mechanical Turks deviates from conventional survey methods. Retrieved from: https://hbz.opus.hbz-nrw.de/opus45-kola/frontdoor/index/index/docId/931.

Schultz, D. P. & Schultz, S. E. (2004). *Theories of personality*. London, United Kingdom: Cengage Learning.

Schultz, D. P. & Schultz, S. E. (2016). *Theories of personality*. London, United Kingdom: Cengage Learning.

Schwartz, H. M. (2017). Club goods, intellectual property rights, and profitability in the information economy. *Business and Politics*, *19*(2), 191–214.

Scott, J. (1983). *Fifty key sociologists: The contemporary theorists*. London, United Kingdom: Routledge.

Sechrest, L. & Sidani, S. (1995). Quantitative and qualitative methods: Is there an alternative? *Evaluation and Program Planning*, *18*(1), 77–87.

Seidman, G. (2013). Self-presentation and belonging on Facebook: How personality influences social media use and motivations. *Personality and Individual Differences*, *54*(3), 402–407.

Sert, S. A., Onur, E., & Yazici, A. (2015). Security attacks and countermeasures in surveillance wireless sensor networks. In *Proceedings of the 9th International Conference on Application of Information and Communication Technologies*, (pp. 201–205). IEEE.

Shan, Y. & King, K. W. (2015). The effects of interpersonal tie strength and subjective norms on consumers' brand-related eWOM referral intentions. *Journal of Interactive Advertising*, *15*(1), 16–27.

Shantz, A. S. (2018). Big data, bigger questions: Data-based business models and their implications for organizational boundaries, data governance, and society. *Toward Permeable Boundaries of Organizations*, *57*, 305–329.

Shapiro, D. C. (2019). Information reporting by cryptocurrency exchanges. *Journal of Taxation of Investments*, *36*(3), 69–77.

Shappie, A. T., Dawson, C. A., & Debb, S. M. (2019). Personality as a predictor of cybersecurity behavior. *Psychology of Popular Media Culture*.

Shattuck, J. (1984). Computer matching is a serious threat to individual rights. *Communications of the ACM*, *27*(6), 538–541.

Shore, J. & Steinman, J. (2015). Did you really agree to that? the evolution of Facebook's privacy policy. *Technology Science*, *8*(11), 1–37.

Shropshire, J., Warkentin, M., Johnston, A., & Schmidt, M. (2006). Personality and IT security: An application of the Five-Factor model. In *Proceedings of the 12th Americas Conference on Information Systems*, (pp. 3443–3449). AIS.

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, *49*, 177–191.

Singh, P. & Singh, M. (2015). Fraud detection by monitoring customer behavior and activities. *International Journal of Computer Applications*, *111*(11).

Singh, S. (2018). Review of Lauer's Creditworthy: A history of consumer surveillance and financial identity in America. *Surveillance & Society*, *16*(1), 134–136.

Siponen, M. & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, *34*(3), 487–502.

Siponen, M. T. (2001). Five dimensions of information security awareness. *SIGCAS Computers and Society*, *31*(2), 24–29.

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.

Smith, B. C., Wright, C., Macdonald, C., et al. (1998). *Knowing our own minds*. Oxford, United Kingdom: Oxford University Press.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, *35*(4), 989–1016.

Snowden, E. (2013). NSA whistleblower Edward Snowden: 'I don't want to live in a society that does these sort of things'. Retrieved from: https://goo.gl/ZthIxV.

Snowden, M. (2016). 'State of Surveillance' with Edward Snowden and Shane Smith. Retrieved from: https://www.youtube.com/watch?v=ucRWyGKBVzo&t=35s.

Snyman, D. & Kruger, H. (2017). Optical polling for behavioural threshold analysis in information security. In *Proceedings of the International Conference on Information and Knowledge Engineering*, (pp. 39–45). CSREA.

Snyman, D., Kruger, H. A., & Kearney, W. D. (2017). The lemming effect in information security. In *Proceedings of the 11th International Symposium on Human Aspects of Information Security & Assurance*, (pp. 91–103). AIS.

Solove, D. J. (2001). Privacy and power: Computer databases and metaphors for information privacy. *Stanford Law Review*, *53*(6), 1393–1462.

Sønderskov, K. M. & Dinesen, P. T. (2016). Trusting the state, trusting each other? the effect of institutional trust on social trust. *Political Behavior*, *38*(1), 179–202.

Srinivasan, D. (2019). The antitrust case against Facebook: A monopolist's journey towards pervasive surveillance in spite of consumers' preference for privacy. *Berkeley Business Law Journal*, *16*(1), 39.

Srivastava, S., John, O. P., Gosling, S. D., & Potter, J. (2003). Development of personality in early and middle adulthood: Set like plaster or persistent change? *Journal of Personality and Social Psychology*, *84*(5), 1041.

Stahl, B. C. (2006). Emancipation in cross-cultural IS research: The fine line between relativism and dictatorship of the intellectual. *Ethics & Information Technology*, *8*(3), 97–108.

Stahl, B. C. (2008). The ethical nature of critical research in information systems. *Information Systems Journal*, *18*(2), 137–163.

Stahl, T. (2016). Indiscriminate mass surveillance and the public sphere. *Ethics and Information Technology*, *18*(1), 33–39.

Staiano, J., Oliver, N., Lepri, B., de Oliveira, R., Caraviello, M., & Sebe, N. (2014). Money walks: A human-centric study on the economics of personal mobile data. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, (pp. 583–594). ACM.

Stavrova, O. & Kokkoris, M. D. (2019). Struggling to be liked: The prospective effect of trait self-control on social desirability and the moderating role of Agreeableness. *International Journal of Psychology*, *54*(2), 232–236.

Stewart, K., Kammer-Kerwick, M., Auchter, A., Koh, H. E., Dunn, M. E., & Cunningham, I. (2019). Examining digital video advertising (DVA) effectiveness: The role of product category, product involvement, and device. *European Journal of Marketing*, *53*(11), 2451–2479.

Stone, M. (1974). Cross-validatory choice and assessment of statistical predictions. *Journal of the Royal Statistical Society: Series B (Methodological)*, *36*(2), 111–133.

Straub, D., Boudreau, M.-C., & Gefen, D. (2004). Validation guidelines for IS Positivist research. *Communications of the Association for Information systems*, *13*(1), 380–427.

Suebsumrarn, P. & Varma, P. (2019). The influence of Extraversion and Neuroticism on self-esteem and life satisfaction mediated by Facebook use among Thai Millennials. *Scholar: Human Sciences*, *11*(1), 191–198.

Sundar, S. S., Kang, H., Wu, M., Go, E., & Zhang, B. (2013). Unlocking the Privacy Paradox: Do cognitive heuristics hold the key? In *CHI'13 Extended Abstracts on Human Factors in Computing Systems*, (pp. 811–816). ACM.

Swanlund, D. & Schuurman, N. (2016). Mechanism matters: Data production for geosurveillance. *Annals of the American Association of Geographers*, *106*(5), 1063–1078.

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.

Taneja, A., Fiore, V., & Fischer, B. (2015). Cyber-slacking in the classroom: Potential for digital distraction in the new age. *Computers & Education*, *82*, 141–151.

Tavakol, M. & Dennick, R. (2011). Making sense of Cronbach's alpha. *International Journal of Medical Education*, *2*, 53.

Tavani, H. T. (1999). Informational privacy, data mining, and the Internet. *Ethics and Information Technology*, *1*(2), 137–145.

The Associated Press (2019). Facebook charged over ad algorithm U.S. officials say discriminates based on home addresses. Retrieved from: https://globalnews.ca/news/5106561/facebook-ad-algorithm-discrimination-housing/.

Thompson, N., McGill, T. J., & Wang, X. (2017). "Security begins at home": Determinants of home computer and mobile device security behavior. *Computers & Security*, *70*, 376–391.

Tsai, H.-y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A Protection Motivation Theory perspective. *Computers & Security*, *59*, 138–150.

Tsay-Vogel, M., Shanahan, J., & Signorielli, N. (2018). Social media cultivating perceptions of privacy: A 5-year analysis of privacy attitudes and self-disclosure behaviors among Facebook users. *New Media & Society*, *20*(1), 141–161.

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 & Security*, *52*, 128–141.

Turow, J., Hennessy, M., & Draper, N. (2018). Persistent misperceptions: Americans' misplaced confidence in privacy policies, 2003–2015. *Journal of Broadcasting & Electronic Media*, *62*(3), 461–478.

Tuten, T. L. & Bosnjak, M. (2001). Understanding differences in web usage: The role of need for cognition and the Five Factor model of personality. *Social Behavior and Personality: An International Journal*, *29*(4), 391–398.

Uldam, J. (2016). Corporate management of visibility and the fantasy of the post-political: Social media and surveillance. *New Media & Society*, *18*(2), 201–219.

van der Schyff, K., Krauss, K., & Kroeze, J. (2018). Facebook and dataveillance: Demonstrating a Multimodal Discourse Analysis. In *Proceedings of the 24th Americas Conference on Information Systems*, (pp. 1–10). AIS.

Van Dijk, T. A. (1998). *Ideology: A multidisciplinary approach*. Los Angeles, United States of America: Sage.

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.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and Protection Motivation Theory. *Information & Management*, *49*(3-4), 190–198.

Vassend, O. & Skrondal, A. (2011). The NEO personality inventory revised (NEO-PI-R): Exploring the measurement structure and variants of the Five-Factor model. *Personality and Individual Differences*, *50*(8), 1300–1304.

Venkatesh, V. & Morris, M. G. (2000). Why don't men ever stop to ask for directions? gender, social influence, and their role in technology acceptance and usage behavior. *MIS Quarterly*, *24*(1), 115–139.

Vickery, J. R. (2015). 'I don't have anything to hide, but...': The challenges and negotiations of social and mobile media privacy for non-dominant youth. *Information, Communication & Society*, *18*(3), 281–294.

Visser, P. S., Krosnick, J. A., & Lavrakas, P. J. (2000). Handbook of research methods in social and personality psychology. In H. T. Reis & C. M. Judd (Eds.), *Survey research* (pp. 223–252). Cambridge, United Kingdom: Cambridge University Press.

Vladlena, B., Saridakis, G., Tennakoon, H., & Ezingeard, 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. In *Proceedings of the 51st Hawaii International Conference on System Sciences*, (pp. 1–10). AIS.

Wallace, L., James, T. L., & Warkentin, M. (2017). How do you feel about your friends? Understanding situational envy in online social networks. *Information & Management*, *54*(5), 669–682.

Walsham, G. (2005). Learning about being critical. *Information Systems Journal*, *15*(2), 111–117.

Wang, C.-C. & Yang, H.-W. (2006). Passion and dependency in online shopping activities. *CyberPsychology & Behavior*, *10*(2), 296–298.

Wang, E. S.-T. (2019). Effects of brand awareness and social norms on user-perceived cyber privacy risk. *International Journal of Electronic Commerce*, *23*(2), 272–293.

Warkentin, M., Johnston, A. C., Shropshire, J., & Barnett, W. D. (2016). Continuance of protective security behavior: A longitudinal study. *Decision Support Systems*, *92*, 25–35.

Warkentin, M., McBride, M., Carter, L., & Johnston, A. (2012). The role of individual characteristics on insider abuse intentions. In *Proceedings of the 18th Americas Conference on Information Systems*, (pp. 1–10). AIS.

Werbin, K. C. (2011). Spookipedia: Intelligence, social media and biopolitics. *Media, Culture & Society*, *33*(8), 1254–1265.

West, J. P. & Bowman, J. S. (2016). Electronic surveillance at work: An ethical analysis. *Administration & Society*, *48*(5), 628–651.

West, S. M. (2019). Data capitalism: Redefining the logics of surveillance and privacy. *Business & Society*, *58*(1), 20–41.

Westin, A. F. (1968). Privacy and freedom. *Washington & Lee Law Review*, *25*(1), 166–170.

Westin, A. F. (1971). *Information technology in a democracy.* Cambridge, United States of America: Harvard University Press.

Westin, A. F. & Baker, M. A. (1973). Databanks in a free society. *ACM SIGCAS Computers and Society*, *4*(1), 25–29.

Wilken, R. (2014). Places nearby: Facebook as a location-based social media platform. *New Media & Society*, *16*(7), 1087–1103.

Williams, E. J., Beardmore, A., & Joinson, A. N. (2017). Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior*, *72*, 412–421.

Willson, M. & Leaver, T. (2015). Zynga's Farmville, social games, and the ethics of big data mining. *Communication Research and Practice*, *1*(2), 147–158.

Wilson, K., Fornasier, S., & White, K. M. (2010). Psychological predictors of young adults' use of social networking sites. *Cyberpsychology, Behavior, and Social Networking*, *13*(2), 173–177.

Winter, S., Neubaum, G., Eimler, S. C., Gordon, V., Theil, J., Herrmann, J., Meinert, J., & Krämer, N. C. (2014). Another brick in the Facebook wall: How personality traits relate to the content of status updates. *Computers in Human Behavior*, *34*, 194–202.

Wisniewski, P., Xu, H., Lipford, H., & Bello-Ogunu, E. (2015). Facebook apps and tagging: The trade-off between personal privacy and engaging with friends. *Journal of the Association for Information Science and Technology*, *66*(9), 1883–1896.

Wisniewski, P. J., Knijnenburg, B. P., & Lipford, H. R. (2017). Making privacy personal: Profiling social network users to inform privacy education and nudging. *International Journal of Human-Computer Studies*, *98*, 95–108.

Wolfe, H. B. (2017). The mobile phone as surveillance device: Progress, perils, and protective measures. *Computer*, *50*(11), 50–58.

Wolfradt, U. & Doll, J. (2001). Motives of adolescents to use the Internet as a function of personality traits, personal and social factors. *Journal of Educational Computing Research*, *24*(1), 13–27.

Wood, D. M. (2007). *Beyond the panopticon? Foucault and surveillance studies*. Burlington, United States of America: Ashgate Burlington.

Wood, D. M. & Mackinnon, D. (2019). Partial platforms and oligoptic surveillance in the smart city. *Surveillance & Society*, *17*(1/2), 176–182.

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.

Yazdanmehr, A. & Wang, J. (2016). Employees' information security policy compliance: A norm activation perspective. *Decision Support Systems*, *92*, 36–46.

Yoon, K., Hoogduin, L., & Zhang, L. (2015). Big data as complementary audit evidence. *Accounting Horizons*, *29*(2), 431–438.

Zhang, L.-f. (2006). Thinking styles and the Big Five personality traits revisited. *Personality and Individual Differences*, *40*(6), 1177–1187.

Zimmer, J. C., Arsal, R. E., Al-Marzouq, M., & Grover, V. (2010). Investigating online information disclosure: Effects of information relevance, trust and risk. *Information & Management*, *47*(2), 115–123.

Žižek, S. (1989). *The sublime object of ideology*. London, United Kingdom: Verso.

Zlatolas, L., Welzer, T., Hölbl, M., Heričko, M., & Kamišalić, A. (2019). A model of perception of privacy, trust, and self-disclosure on online social networks. *Entropy*, *21*(8), 772.

Zlatolas, L. N., Welzer, T., Heričko, M., & Hölbl, M. (2015). Privacy antecedents for SNS self-disclosure: The case of Facebook. *Computers in Human Behavior*, *45*, 158–167.

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*(1), 75–89.

APPENDIX A

Questionnaires

This appendix contains all the items that comprised both the pilot and final questionnaire of this study. Tables 1 through 16 contain sets of items with each set of items appearing on a separate page of the final survey. The exception here being the personality trait items which are split over five tables. Item loadings denoted with a (d) were dropped to improve convergent validity. Additionally, although items related to social desirability, Facebook usage, and Facebook and PC experience are presented here, these were not used as part of the multivariate analysis. Hence, the absence of values for the mean, standard deviation (SD) and factor loadings in these instances. To view the actual SurveyMonkey-hosted questionnaires use the link supplied in the footnote [1].

Table 2: Questionnaire's demographic items

	Item	**Source**	**Response anchors**
2	What is your age?	SurveyMonkey	0 = 18-24, 1 = 25-34, 2 = 35-44, 3 = 45-54, 4 = 55-64, 5 = 65-74, 6 = 75 or older
3	What is your gender?	SurveyMonkey	Female / Male
4	What is the highest level of education you have completed?	Symeonidis et al., (2018)	No degree or up to high school, Bachelors or equivalent, Masters degree and above

[1] https://bit.ly/37L3iOo

Table 3: Questionnaire items related to Facebook usage

	Item	Source	Mean	SD	Loading	Response anchors
5	Approximately how many total Facebook friends do you have?	Ellison et al., (2007)	5.47	2.54	0.261(d)	0 = 10 or less, 1 = 11-50, 2 = 51-100, 3 = 101-150, 4 = 151-200, 5 = 201-250, 6 = 251-300, 7 = 301-400, 8 = more than 400
6	In the past week, on average, approximately how many minutes per day have you spent on Facebook?	Ellison et al., (2007)	2.97	1.45	0.620	0 = less than 10, 1 = 10-30, 2 = 31-60, 3 = 1-2 hours, 4 = 2-3 hours, 5 = more than 3 hours
7	Facebook is part of my everyday activity.	Ellison et al., (2007)	2.18	1.15	0.915	Strongly disagree, Disagree, Neither agree nor disagree, Agree, Strongly Agree
8	I am proud to tell people I'm on Facebook.	Ellison et al., (2007)	2.89	1.02	0.686	Strongly disagree, Disagree, Neither agree nor disagree, Agree, Strongly Agree
9	Facebook has become part of my daily routine.	Ellison et al., (2007)	2.23	1.14	0.918	Strongly disagree, Disagree, Neither agree nor disagree, Agree, Strongly Agree
10	I feel out of touch when I haven't logged onto Facebook for a while.	Ellison et al., (2007)	2.80	1.29	0.731	Strongly disagree, Disagree, Neither agree nor disagree, Agree, Strongly Agree
11	I feel I am part of the Facebook community.	Ellison et al., (2007)	2.62	1.18	0.749	Strongly disagree, Disagree, Neither agree nor disagree, Agree, Strongly Agree
12	I would be sorry if Facebook shut down.	Ellison et al., (2007)	2.83	1.36	0.738	Strongly disagree, Disagree, Neither agree nor disagree, Agree, Strongly Agree
13	How many Facebook Apps have you used in the past?	Adapted from Symeonidis et al., (2018)	2.32	1.56	0.155(d)	0 = 1-2, 1 = 3-4, 2 = 5-6, 3 = 7-8, 4 = more than 9, 5 = unknown
14	I intend to continue using Facebook Apps.	Adapted from Lankton, McKnight and Tripp (2017); Warkentin et al. (2016)	2.38	1.10	0.501	Extremely unlikely, Unlikely, Neutral, Likely, Extremely likely

Table 4: Questionnaire items related to Facebook and PC experience

	Item	Source	Response anchors
15	I feel confident using Facebook Apps.	(Saridakis et al., 2016)	Strongly disagree, Disagree, Neither agree nor disagree, Agree, Strongly Agree
16	I feel confident understanding terms/words relating to Facebook Apps.	(Saridakis et al., 2016)	Strongly disagree, Disagree, Neither agree nor disagree, Agree, Strongly Agree
17	I feel confident working on a personal computer.	(Saridakis et al., 2016)	Strongly disagree, Disagree, Neither agree nor disagree, Agree, Strongly Agree

Table 5: Questionnaire's first attention trap item

	Item	Source	Response anchor
18	What is the answer to the following equation: (10+10)x2?	New	0 = 2, 1 = 30, 2 = 20, 3 = 40, 4 = 10

Table 6: Questionnaire items of the *personality constructs (1 of 5)*

	Item	Source	Mean	SD	Loading	t-statistic	Response anchors
19	I see myself as someone who is talkative.	John and Srivastava (1999)	2.86	1.36	0.788	40.89***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree
20	I see myself as someone who tends to find fault with others.	John and Srivastava (1999)	3.50	1.25	0.740	28.92***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree
21	I see myself as someone who does a thorough job.	John and Srivastava (1999)	1.46	.742	0.674	25.18***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree
22	I see myself as someone who is depressed, blue	John and Srivastava (1999)	3.83	1.31	0.667	25.64***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree
23	I see myself as someone who is original, comes up with new ideas.	John and Srivastava (1999)	2.08	1.04	0.792	39.61***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree
24	I see myself as someone who is reserved.	John and Srivastava (1999)	2.38	1.26	0.764	35.82***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree
25	I see myself as someone who is helpful and unselfish with others.	John and Srivastava (1999)	1.86	.887	0.612	19.06***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree
26	I see myself as someone who can be somewhat careless.	John and Srivastava (1999)	3.73	1.23	0.682	25.83***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree
27	I see myself as someone who is relaxed, handles stress well.	John and Srivastava (1999)	2.25	1.25	0.851	58.42***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree
28	I see myself as someone who is curious about many different things.	John and Srivastava (1999)	1.65	.830	0.599	19.41***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree

Table 7: Questionnaire items of the *personality constructs (2 of 5)*

	Item	Source	Mean	SD	Loading	t-statistic	Response anchors
29	I see myself as someone who is full of energy.	John and Srivastava (1999)	2.53	1.22	0.563	17.34***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree
30	I see myself as someone who starts quarrels with others.	John and Srivastava (1999)	4.35	.959	0.553	16.01***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree
31	I see myself as someone who is a reliable worker.	John and Srivastava (1999)	1.41	.707	0.659	22.88***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree
32	I see myself as someone who can be tense.	John and Srivastava (1999)	3.10	1.31	0.692	28.11***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree
33	I see myself as someone who is ingenious, a deep thinker.	John and Srivastava (1999)	2.18	1.10	0.716	29.40***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree
34	I see myself as someone who generates a lot of enthusiasm.	John and Srivastava (1999)	2.59	1.25	0.616	20.60***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree
35	I see myself as someone who has a forgiving nature.	John and Srivastava (1999)	2.10	1.22	0.624	20.60***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree
36	I see myself as someone who tends to be disorganized.	John and Srivastava (1999)	3.82	1.25	0.727	30.24***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree
37	I see myself as someone who worries a lot.	John and Srivastava (1999)	3.02	1.43	0.770	38.71***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree

Table 8: Questionnaire items of the *personality constructs (3 of 5)*

	Item	Source	Mean	SD	Loading	t-statistic	Response anchors
38	I see myself as someone who has an active imagination.	John and Srivastava (1999)	1.92	1.02	0.652	23.35***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree
39	I see myself as someone who tends to be quiet.	John and Srivastava (1999)	2.50	1.35	0.811	44.05***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree
40	I see myself as someone who is generally trusting.	John and Srivastava (1999)	2.30	1.26	0.508	13.93***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree
41	I see myself as someone who tends to be lazy.	John and Srivastava (1999)	3.88	1.20	0.715	29.36***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree
42	I see myself as someone who is emotionally stable, not easily upset.	John and Srivastava (1999)	2.18	1.23	0.827	51.41***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree
43	I see myself as someone who is inventive.	John and Srivastava (1999)	2.28	1.13	0.724	30.08***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree
44	I see myself as someone who has an assertive personality.	John and Srivastava (1999)	2.86	1.33	0.592	19.39***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree
45	I see myself as someone who can be cold and aloof.	John and Srivastava (1999)	3.53	1.27	0.699	25.97***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree

Table 9: Questionnaire items of the *personality constructs (4 of 5)*

	Item	Source	Mean	SD	Loading	t-statistic	Response anchors
46	I see myself as someone who perseveres until the task is finished.	John and Srivastava (1999)	1.71	.920	0.724	30.03***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree
47	I see myself as someone who can be moody.	John and Srivastava (1999)	3.26	1.37	0.686	27.54***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree
48	I see myself as someone who values artistic, aesthetic experiences.	John and Srivastava (1999)	1.96	1.06	0.601	19.44***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree
49	I see myself as someone who is sometimes shy, inhibited.	John and Srivastava (1999)	2.72	1.40	0.753	35.08***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree
50	I see myself as someone who is considerate and kind to almost everyone.	John and Srivastava (1999)	1.76	.919	0.683	24.17***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree
51	I see myself as someone who does things efficiently.	John and Srivastava (1999)	1.63	.802	0.713	29.16***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree
52	I see myself as someone who remains calm in tense situations.	John and Srivastava (1999)	2.11	1.12	0.725	31.91***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree
53	I see myself as someone who prefers work that is routine.	John and Srivastava (1999)	2.56	1.27	0.373(d)	9.32***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree
54	I see myself as someone who is outgoing, sociable.	John and Srivastava (1999)	2.86	1.39	0.805	43.95***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree

Table 10: Questionnaire items of the *personality constructs (5 of 5)*

	Item	Source	Mean	SD	Loading	t-statistic	Response anchors
55	I see myself as someone who is sometimes rude to others.	John and Srivastava (1999)	3.93	1.14	0.705	26.00***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree
56	I see myself as someone who makes plans and follows through with them.	John and Srivastava (1999)	1.71	.907	0.665	24.47***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree
57	I see myself as someone who gets nervous easily.	John and Srivastava (1999)	3.25	1.42	0.807	46.36***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree
58	I see myself as someone who likes to reflect, play with ideas.	John and Srivastava (1999)	2.01	1.05	0.732	31.22***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree
59	I see myself as someone who has few artistic interests.	John and Srivastava (1999)	3.63	1.31	0.449(d)	11.97***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree
60	I see myself as someone who likes to cooperate with others.	John and Srivastava (1999)	1.88	.931	0.498(d)	13.68***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree
61	I see myself as someone who is easily distracted.	John and Srivastava (1999)	3.63	1.28	0.565	14.03***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree
62	I see myself as someone who is sophisticated in art, music, or literature.	John and Srivastava (1999)	2.57	1.25	0.590	18.84***	Disagree strongly, Disagree a little, Neither agree nor disagree, Agree a little, Strongly Agree

Table 11: Questionnaire's second attention trap item

	Item	Source	Response anchor
63	What is the answer to the following equation: (7 x 3)+1?	New	0 = 22, 1 = 23, 2 = 21, 3 = 28, 4 = 30

Table 12: Questionnaire items of the construct *Attitude towards privacy*

	Item	Source	Mean	SD	Loading	t-statistic	Response anchors
64	It is risky to use Facebook apps.	Adapted from Parsons et al., (2017)	2.91	1.08	0.191(d)	4.06***	Strongly disagree, Disagree, Neither agree nor disagree, Agree, Strongly Agree
65	Using the privacy settings on my Facebook account is unnecessary.	Adapted from Taneja, Vitrano and Gengo (2014)	4.33	.88	0.707	25.69***	Strongly disagree, Disagree, Neither agree nor disagree, Agree, Strongly Agree
66	Using the privacy settings on my Facebook account is important.	Adapted from Taneja, Vitrano and Gengo (2014)	1.47	.747	0.821	33.42***	Strongly disagree, Disagree, Neither agree nor disagree, Agree, Strongly Agree
67	Using the privacy settings on my Facebook account is good.	Adapted from Taneja, Vitrano and Gengo (2014)	1.45	.656	0.762	29.09***	Strongly disagree, Disagree, Neither agree nor disagree, Agree, Strongly Agree
68	It is important that Facebook Apps have access to my personal information.	New	3.82	1.09	0.381(d)	8.11***	Strongly disagree, Disagree, Neither agree nor disagree, Agree, Strongly Agree
69	It is good that Facebook Apps have access to my personal information.	New	4.00	1.02	0.415(d)	8.92***	Strongly disagree, Disagree, Neither agree nor disagree, Agree, Strongly Agree
70	It is unnecessary for Facebook Apps to have access to my personal information.	New	1.89	1.02	0.376(d)	8.41***	Strongly disagree, Disagree, Neither agree nor disagree, Agree, Strongly Agree

Table 13: Questionnaire items of the construct *Social norms*

	Item	Source	Mean	SD	Loading	t-statistic	Response anchors
71	I am likely to use a Facebook app if my family and/or friends also use the app.	New	2.68	1.13	0.575	17.91***	Strongly disagree, Disagree, Neither agree nor disagree, Agree, Strongly Agree
72	Most of my friends are using Facebook apps.	Adapted from Ramayah, Rouibah and Rangle (2009)	2.20	.962	0.856	49.11***	Strongly disagree, Disagree, Neither agree nor disagree, Agree, Strongly Agree
73	Most of my family are using Facebook apps.	Adapted from Ramayah, Rouibah and Rangle (2009)	2.38	1.06	0.783	38.05***	Strongly disagree, Disagree, Neither agree nor disagree, Agree, Strongly Agree
74	Most people I know are using Facebook apps.	Adapted from Ramayah, Rouibah and Rangle (2009)	2.26	.983	0.857	48.78***	Strongly disagree, Disagree, Neither agree nor disagree, Agree, Strongly Agree
75	Friends who influence my behaviour think that I should use Facebook apps.	Adapted from Thompson, McGill and Wang (2017)	3.23	1.14	0.662	21.39***	Strongly disagree, Disagree, Neither agree nor disagree, Agree, Strongly Agree
76	Significant others who are important to me think that I should use Facebook apps.	Adapted from Thompson, McGill and Wang (2017)	3.23	1.14	0.653	20.56***	Strongly disagree, Disagree, Neither agree nor disagree, Agree, Strongly Agree
77	My peers think that I should use Facebook apps.	Adapted from Thompson, McGill and Wang (2017)	3.05	1.08	0.699	24.39***	Strongly disagree, Disagree, Neither agree nor disagree, Agree, Strongly Agree

Table 14: Questionnaire items of the construct *Information security awareness (1 of 2)*

	Item	**Source**	**Mean**	**SD**	**Loading**	**t-statistic**	**Response anchors**
78	Playing online games on Facebook.	Ögütçü et al. (2016)	3.56	1.00	0.210(d)	4.91***	Too dangerous, Dangerous, Less dangerous, Safe, No idea
79	I must periodically review the privacy settings on my Facebook account.	Adapted from Parsons et al. (2017)	1.91	.997	0.503	14.85***	Strongly disagree, Disagree, Neither agree nor disagree, Agree, Strongly Agree
80	It is very important to me that I am aware and knowledgeable about how my personal information will be used.	Hallam et al., (2017)	1.58	.758	0.544	17.03***	Strongly disagree, Disagree, Neither agree nor disagree, Agree, Strongly Agree
81	Companies seeking information online should disclose the way the data are collected, processed and used.	Hallam et al., (2017)	1.33	.662	0.458(d)	12.86***	Strongly disagree, Disagree, Neither agree nor disagree, Agree, Strongly Agree
82	I follow the news and developments about the privacy issues and privacy violations related to social media.	Adapted from Xu et al., (2008)	2.11	1.00	0.378(d)	9.78***	Strongly disagree, Disagree, Neither agree nor disagree, Agree, Strongly Agree
83	I am aware of the privacy issues related to the use of Facebook apps.	Adapted from Xu et al., (2008)	1.92	.898	0.320	7.92***	Strongly disagree, Disagree, Neither agree nor disagree, Agree, Strongly Agree

Table 15: Questionnaire items of the construct *Information security awareness (2 of 2)*

	Item	Source	Mean	SD	Loading	t-statistic	Response anchors
84	I believe I have control over who can get access to my personal information collected by Facebook apps.	Adapted from Xu et al., (2008)	2.93	1.21	0.186	4.32***	Strongly disagree, Disagree, Neither agree nor disagree, Agree, Strongly Agree
85	The default privacy settings on Facebook allow my friend's apps to collect my information.	Symeonidis et al., (2018)	3.47	1.27	0.803	47.07***	Not at all concerned, Slightly concerned, Somewhat concerned, Moderately concerned, Extremely concerned
86	Facebook does not notify me in advance of the possibility that one of my friend's apps is going to collect information about me.	Symeonidis et al., (2018)	3.73	1.24	0.897	84.22***	Not at all concerned, Slightly concerned, Somewhat concerned, Moderately concerned, Extremely concerned
87	Facebook does not notify me in advance of the possibility that one of my apps is going to collect information about my friends.	Symeonidis et al., (2018)	3.73	1.19	0.872	70.61***	Not at all concerned, Slightly concerned, Somewhat concerned, Moderately concerned, Extremely concerned
88	Facebook does not ask for my approval in advance of the possibility that one of my friend's apps is going to collect information about me.	Symeonidis et al., (2018)	3.83	1.22	0.890	80.42***	Not at all concerned, Slightly concerned, Somewhat concerned, Moderately concerned, Extremely concerned
89	A Facebook app (mydigitallife) was identified as the source of personal information that was abused by Cambridge Analytica.	New	3.85	1.27	0.654	24.85***	Not at all concerned, Slightly concerned, Somewhat concerned, Moderately concerned, Extremely concerned

Table 16: Questionnaire items related to *Social desirability*

	Item	**Source**	**Response anchors**
90	Are you always courteous, even to people who are disagreeable?	(Ray, 1984)	Yes, Unsure, No
91	Are you always a good listener, no matter whom you are talking to?	(Ray, 1984)	Yes, Unsure, No
92	Are you quick to admit making a mistake?	(Ray, 1984)	Yes, Unsure, No
93	Have there been occasions when you took advantage of someone?	(Ray, 1984)	Yes, Unsure, No
94	Do you sometimes try to get even rather than forgive and forget?	(Ray, 1984)	Yes, Unsure, No
95	Do you sometimes feel resentful when you do not get your own way?	(Ray, 1984)	Yes, Unsure, No
96	Are you always willing to admit when you make a mistake?	(Ray, 1984)	Yes, Unsure, No
97	Have you sometimes taken unfair advantage of another person?	(Ray, 1984)	Yes, Unsure, No

APPENDIX B

Research outputs

The following conference paper was developed as a proof-of-concept and presented at the 2018 IFIP 8.11/11.13 Dewald Roode Information Security Research Workshop. This paper is aligned with Chapter 1 and parts of the research model illustrated in Chapter 6:

> van der Schyff, K., Flowerday, S., 2018. **The development of a personality-driven social media dataveillance behaviour model for South Africa.** In Proceedings of the 2018 IFIP 8.11/11.13 Dewald Roode Information Security Research Workshop, Cape Town

Following the aforementioned proof-of-concept, a conceptual journal article was authored. The objective was to receive feedback regarding the novel aspect of this study - the inclusion of the construct named *Information security awareness* instead of *Perceived behavioural control*. It was also used to formally develop some initial thoughts on how an individual's personality traits could influence their intention to use Facebook apps. At this stage the research model and content had undergone a number of minor changes. For example, the term dataveillance was removed based on the feedback received at the Dewald Roode workshop. This article is aligned with Chapter 1 and touches on some aspects of Chapter 3, 4 and 5. Parts of the research model illustrated in Chapter 6 can be found in 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), 1-9

The following journal was written to convey the main findings and structural model of this study; specifically the vulnerability of certain personality traits with regards to Facebook App surveillance:

> van der Schyff, K., Flowerday, S., Lowry, P.B., 2020. **Privacy Behavior in the Use of Facebook Apps: A Personality-based Perspective** *Computers in Human Behavior* [under review]

The following two journal articles were written to as part of an analysis focused on the additional data that was collected. These analyses were primarily focused on the constructs that did not form part of the multivariate analysis or the historical context supporting the thesis problem:

> van der Schyff, K., Flowerday, S., Furnell, S., 2020. **Duplicitous Social Media and Data Surveillance: An evaluation of privacy risk** *Computers & Security* [under review]

> van der Schyff, K., Flowerday, S., Furnell, S., 2020. **Privacy Risk and the Use of Facebook Apps: A gender-based vulnerability** *Computers & Security* [under review - revision 2]

APPENDIX C

Additional statistics

This appendix provides additional statistical results related to the content presented in Chapter 7. Tables C.1 through C.10 are specifically focused on the Variance Inflation Factor (VIF) values which are used to check for multicollinearity.

Table 17: VIF values associated with the construct *Extraversion*

Item	Variance Inflation Factor (VIF)
19	2.83
24	2.90
29	2.48
34	2.89
39	3.49
44	2.03
49	2.86
54	3.03

Table 18: VIF values associated with the construct *Agreeableness*

Item	Variance Inflation Factor (VIF)
20	2.13
25	2.30
30	1.96
35	1.99
40	1.82
45	2.23
50	2.54
55	2.56

Table 19: VIF values associated with the construct *Conscientiousness*

Item	Variance Inflation Factor (VIF)
21	2.30
26	2.30
31	2.12
36	2.67
41	2.46
46	2.42
51	2.35
56	2.09

Table 20: VIF values associated with the construct *Neuroticism*

Item	Variance Inflation Factor (VIF)
22	2.40
27	3.75
32	2.34
37	2.82
42	3.17
47	2.52
52	2.66
57	3.55

Table 21: VIF values associated with the construct *Openness to Experience*

Item	Variance Inflation Factor (VIF)
23	2.86
28	1.84
33	2.39
38	1.92
43	2.45
48	1.98
58	2.34
62	1.83

Table 22: VIF values associated with the construct *Attitude towards privacy*

Item	Variance Inflation Factor (VIF)
65	1.98
66	2.82
67	2.74

Table 23: VIF values associated with the construct *Social norms*

Item	Variance Inflation Factor (VIF)
71	2.04
72	4.02
73	2.77
74	4.02
75	3.01
76	3.42
77	3.25

Table 24: VIF values associated with the construct *Information security awareness*

Item	Variance Inflation Factor (VIF)
79	1.74
80	2.00
85	2.98
86	4.53
87	4.36
88	4.52
89	2.07