An Online Information Security Awareness Model: The Disclosure of Personal Data

by

Heather Joubert Parker

ORCID: https://orcid.org/0000-0003-0653-1497

An Online Information Security Awareness Model: The Disclosure of Personal Data.

By

Heather Joubert Parker

15P0295

THESIS

submitted in fulfilment of the requirements for the degree

MASTER OF COMMERCE

In

INFORMATION SYSTEMS

in the

FACULTY OF COMMERCE

of

Rhodes University

Supervisor: **Prof. Stephen Flowerday**

November 2020

ABSTRACT

Social media has revolutionized the way people send and receive information by creating a new level of interconnected communication. However, the use of the Internet and social media brings about various ways in which a user's personal data can be put at risk. This study aims to investigate what drives the disclosure of personal information online and whether an increase in awareness of the value of personal information motivates users to safeguard their information. Fourteen university students participated in a mixed-methods experiment, where they completed a questionnaire before and after being shown the data stored about them by online platforms to determine if changes occur in their intention to disclose. Following completing the initial questionnaire, the participant viewed the personal data stored about them by Facebook, Google, and Instagram. Other online tools such as Social Profile Checker, Facebook View As, and HaveIBeenPawned were used to see the information publicly available about each participant. Together these findings were discussed in a semi-structured interview to determine the influence of attitudes, subjective norms, and awareness on the cost-benefit analysis users conduct when disclosing information online. Overall, the findings indicate that users are able to disregard their concerns due to a resigned and apathetic attitude towards privacy. Furthermore, subjective norms enhanced by FOMO further allow users to overlook potential risks to their information in order to avoid social isolation and sanction. Alternatively, an increased awareness of the personal value of information and having experienced a previous privacy violation encourage the protection of information and limited disclosure. Thus, this study provides insight into privacy and information disclosure on social media in South Africa. It reveals more insight into the cost-benefit analysis users conduct by combining the Theory of Planned Behaviour with the Privacy Calculus Model, as well as the antecedent factors of *Trust in the Social Media Provider*, *FOMO,* and *Personal Valuation of Information.*

KEYWORDS: Information Disclosure; Privacy Calculus; Online Risk; Social Media; Theory of Planned Behaviour; Awareness; FOMO.

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 clearance number 2020-0872-3206.

_____

Date

ACKNOWLEDGEMENTS

I would like to thank my supervisor, Professor Stephen Flowerday, for his guidance and constructive feedback during the development of this thesis. I would also like to thank the NRF and The Allan Gray Scholarship for their financial support. Finally, I would like to thank my family and friends for their motivation and encouragement.

GLOSSARY

Term	Definition
Social Media	A collection of websites and applications that are used from sharing content, communication, collaboration, and interaction (Rouse, 2016).
Self-Disclosure	Revealing information of a personal nature to others (Varnali & Toker, 2015).
Trust	"The firm belief in the competence of an entity to act dependably, securely and reliably within a specified context" (Grandison & Sloman, 2000)
Attitude	Attitude refers to the extent to which an individual considers performing a specific behaviour as either being positive or negative (Ajzen, 1991).
Subjective Norms	"The perceived social pressure to perform or not perform the behaviour" (Ajzen, 1991, p. 188).
Fear of Missing Out (FOMO)	"Defined as a pervasive apprehension that others might be having rewarding experiences from which one is absent, FOMO is characterized by the desire to stay continually connected with what others are doing" (Przybylski, et al., 2013, p. 1841)
Optimism Bias	"Many people judge themselves to be less at risk for various hazards when they compare themselves with others" (Siegrist & Árvai, 2020, p. 1247)
Data vs Information	Data is defined as raw fact, and information is processed data to create meaning (Zins, 2007). In the context of this study data and information are used interchangeably.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1: INTRODUCTION

1.1 Background

Social media has evolved from merely being a pastime to one of the main modes of communication and an important part of daily life (Mohamed-Ahmed, 2015). Furthermore, 3.96 billion people are social media users, which is more than half the world's population (Kemp, 2020). The average user spends six and a half hours online daily, with two hours and 22 minutes a day spent on social media (Kemp, 2020). This regular engagement and disclosure online enable cybercriminals to piece together a comprehensive picture of an intended victim's life, which allows them to effectively target their victims (Middleton-Leal, 2019).

Users feel the need to disclose information to foster relationships because society relies on communication. Social media provides the perfect platform to manage these relationships by sharing life events and other personal information to keep friends and followers informed. During the recent COVID-19 pandemic, people have been engaging on social media far more to compensate for not being able to physically see their friends and family (Nabity-Grover, Cheung & Thatcher, 2020). Topics for disclosure have also changed during this time, as posting about social gatherings and dining out is frowned upon, while disclosure about one's health status is becoming more prevalent (Nabity-Grover, et al., 2020). Cybersecurity threats have also increased during this time, with cybercriminals using information about COVID-19 as a lure to instigate phishing attacks (Gollin, 2020). Thus, while users enjoy the benefits of their engagement on social media, they are unavoidably exposed to privacy and security threats (Feng, et al., 2019).

Additionally, the nature of privacy is more complex online, as many non-verbal cues available to people in real life are not available in online communication (Tsay-Vogel, Shanahan & Signorielli, 2018). This encourages users to disclose more information to off-set the lack of cues such as body language and vocal tone. Furthermore, in offline contexts protecting privacy is commonplace, however, online users do not often perform equivalent preventative behaviours to protect their privacy and arguably leave the doors to their online identity unlocked (Bartsch & Dienlin, 2016). For instance, many users often stick to default privacy settings because they are thought of as indirect recommendations (Acquisti, et al.,

2015). Platforms use these settings to their advantage by setting defaults to encourage disclosure and profile visibility (Acquisti, et al., 2015). These privacy settings also change frequently, which make it difficult for users to remain updated on how best to use them (McPeak, 2013).

Moreover, the privacy policies of platforms such as Google, Facebook, and Instagram stipulate what information is collected about users. However, since many users do not read these policies, they remain unaware of the exact personal data collected, stored, and shared with third parties (Esteve, 2017). For example, the scope of data collected by these platforms is far more comprehensive than users might realise, as online platforms also compile data not deliberately posted by users (McPeak, 2013). Users are further limited when they lack an understanding of the value their data has, both from a personal and economic point of view.

Given that personal data is a sought-after commodity with significant economic value (Esteve, 2017), it seems plausible that an increased understanding of the personal value a user attaches to their data might motivate them to engage more cautiously online.

1.2 Problem Statement

Social media has become a primary form of communication, and its very nature urges users to share intimate details of their lives to a broad online audience. The benefits users gain from this constant connection to others comes at a price, as the increased accessibility of the Internet has launched new avenues for fraud and crime that expose millions of users to global cyber-criminals (Thompson, McGill & Wang, 2017). While cyber-threats and criminals have adapted, the user's ability to manage online threats to their personal information have not kept up the pace. For instance, users lack knowledge surrounding how to most effectively employ methods to protect themselves online (Nyoni & Velempini, 2015). In line with this, users are often unaware of how their information is harvested and used by online platforms ((Benson, Saridakis. & Tennakoon, 2015; Barth & De Jong, 2017). While few users grasp the personal value they assign to their information, once they think of their personal information as a tradeable asset, they become more hesitant to share this data (Spiekermann, Korunovska & Bauer, 2012). This points to the notion that users seldom understand the full implications of disclosing vast amounts of information online.

Taking the above problem background into account, the problem statement of this thesis is as follows:

> **People remain unaware of the value of their online personal data and how this data is harvested, stored, and used by third parties. Due to this lack of awareness, users often disclose vast amounts of personal information on social media without realising the security risk this disclosure poses. Thus, their online privacy is potentially compromised.**

1.3 Research Questions

Based on the background and problem statement, this research intends to review the factors that influence a user to disclose personal information online. This includes investigating whether an increase in awareness of the value of personal information could influence a user to safeguard their personal information. Consequently, this study will be significant to all Internet users who wish to secure their personal information online by increasing their awareness of the value of their personal data.

To facilitate this, the main research question is stated as follows:

> **How does awareness, attitudes, and subjective norms influence the cost-benefit analysis users conduct when deciding to disclose personal information online?**

The research sub-questions are as follows:

a) *How does the Privacy Calculus influence information disclosure online?*

   The purpose of this question is to examine the influence of the Privacy Calculus on information disclosure.

b) *How does attitude towards disclosure influence the cost-benefit analysis users conduct when disclosing information?*

   The goal of this question is to determine how attitude affects risk and benefit perception.

c) *What factors influence a user's attitude towards sharing personal information online?*

This question aims to establish the factors that influence a user's attitude towards disclosing personal information.

d) *How does subjective norms influence a user's intention to disclose personal information online?*

   This question aims to establish how subjective norms influence risk and benefit perception and, in so doing, intention to disclose personal information.

e) *How does information security awareness of the value of personal data influence perceived control over self-disclosure behaviour online?*

   The goal of this question is to determine what effect an increase in awareness of the value of personal information has on a user's intention to disclose personal information online.

1.4 Research Objective

Users can share, like, comment, and post anytime, day or night, as social media and the Internet provide 24/7 access to information, entertainment, and other content. This constant online engagement has become a daily habit that poses various threats to a user's data privacy and security (Barth & De Jong, 2017). Yet, users continue to willingly disclose personal information online. As such, it would be useful to gain new insight into what drives users to disclose personal information online despite the potential risks.

Taking this into account, the main objective of this study is as follows:

To understand how attitude, subjective norms, and awareness influence a user's perception of the benefits and risks associated with information disclosure and, in turn, their intention to disclose personal information online.

1.5 Initial Literature Review

The following initial literature review was conducted during the proposal phase of the study. It was intended to sketch the background to the study and provide an idea of the prominent theories and literature related to the study.

1.5.1 Factors influencing Information Disclosure

People from all walks of life use the Internet to engage in various activities ranging from work to entertainment. At the same time, social media has become an essential medium for

communication. However, a considerable dark side exists to engaging on these sites that put a user's personal information at risk (Fox & Moreland, 2015). As such, it is imperative to understand the main factors that influence online information disclosure, specifically awareness, privacy attitude, social norms, perceived risk, and perceived benefit (Jafarkarimi, et al., 2016; Krasnova, Kolesnikova. & Günther, 2009; Nyoni & Velempini, 2018; Xu, Michael. & Chen, 2013; Zlatolas, et al., 2015).

Users are unaware of the consequences and abuse of the information they disclose online (Acquisti, et al., 2015). For instance, users are unaware of the personal data that they give to Facebook and Google and may be unaware of the personal data that is automatically collected about them via these platforms (Esteve, 2017). This lack of awareness results in users trustingly disclosing their personal information. Nyoni and Velempini (2018), revealed that users are unaware that their movements and activities can be tracked via the personal data that they post to the public domain. This study also noted that privacy awareness among users must be increased to "protect them from possible loss of property or surveillance" (Nyoni & Velempini, 2018). Existing literature on security and privacy consists of studies conducted in the corporate environment (Saridakis, et al., 2015). Thus, there is a need to investigate individual information disclosure behaviour and awareness.

Previous research has investigated various factors related to information disclosure intention, including privacy concerns, personality traits, privacy risks, social benefits, and psychological states (Abramova, et al., 2017). However, little research has been done on a user's awareness of their personal valuation of information (Spiekermann & Korunovska, 2017). While various studies have investigated the influence of the monetary value of personal data on privacy (Bauer, Korunovska & Spiekermann, 2012; Malgieri & Custers, 2018; Spiekermann & Korunovska, 2017; Wagner, et al., 2018), new insight could be gained from examining the effects of personal valuation of information on a user's willingness to disclose personal information online.

Studies have found that privacy concerns have a positive effect on privacy attitudes and intentions, which has a positive influence on privacy-related behaviours (Kokolakis, 2017). Furthermore, a positive attitude towards online privacy increases a user's privacy concerns (Jakovljević, 2011). Thus, privacy attitude is a strong predictor of actual privacy behaviour (Gerber, Gerber & Volkamer, 2018). Another aspect of privacy-related research refers to

the privacy paradox, where inconstancies exist between a person's attitude and behaviour (Barth & De Jong, 2017). Users often claim they care about the privacy of their information, but they will reveal personal data for small rewards (Kokolakis, 2017).

A user's attitude is often influenced by the social norms surrounding information privacy and disclosure. It has been suggested that public opinion is important when it comes to an individual's privacy valuation (Laufer & Wolfe, 1977). Social norms can influence a user's self-disclosure behaviour because they feel pressured to respond in a certain way (Dienlin & Trepte, 2015). Thus, a user's actual behaviour reflects public opinion, and the user's attitude refers to their unbiased opinion (Dienlin & Trepte, 2015; Gerber, et al., 2018). Social norms significantly influence intention to use privacy controls (Taneja, Vitrano & Gengo, 2014), and subjective norms have been found to predict the use of social networking sites (Varnali & Toker, 2015).

To understand information disclosure online, some studies have used the Theory of Planned Behaviour (Heirman, Walrave & Ponnet, 2013; Kim, et al., 2016). The Theory of Planned Behaviour proposes that behaviour is influenced by attitude, subjective norms, and perceived behavioural control (Ifinedo, 2012). Xu, et al. (2013), proposed an integrated model combining the Theory of Planned Behaviour and the perceived benefit construct from the Privacy Calculus Theory to explain information disclosure on social media sites.

The Privacy Calculus Theory has also been applied to previous studies on information disclosure to clarify why users are willing to disclose their personal information online (Krasnova, et al., 2010). This theory argues that the returns of information disclosure balance the risk of the user's privacy being compromised (Dinev & Hart, 2006). Consequently, a loss of privacy is the price one pays for the benefits acquired by disclosing personal information (Hui, Tan, & Goh, 2006). Gerber, et al. (2018), found substantial evidence for the use of the Privacy Calculus theoretical framework when determining information disclosure. Studies using the Privacy Calculus Theory focused on the effect of perceived benefits and perceived costs on information disclosure and self-disclosure on social media (Cheung, et al., 2015). Perceived benefits are one of the strongest predictors of intention to disclose personal information and in the context of social media, these benefits refer to increasing social capital (Gerber, et al., 2018). Thus, the rewards gained from

engaging on social media platforms can surpass the privacy risks and cause users to disclose information (Krasnova, et al., 2010).

Various other theories have been applied to evaluate the factors influencing information disclosure online. The research done by Mamonov and Benbunan-Fich (2018), used the Information Processing framework to examine the degree to which users would disclose personal information once they were exposed to reports of security breaches. The Protection Motivation Theory has also been used to determine why users carry out protective behaviours and proposes that protective behaviour is motivated by coping and threat assessments (Tsai, et al., 2016).

The above initial literature review has highlighted that many individuals are unaware of the data collected about them, as well as being unaware of the personal value of this data. Therefore, there is a need to examine the influence of an individual's awareness of personal information security on their online behaviour and their willingness to disclose personal information.

1.6 Methodological Approach

This study explored the research problem using the interpretivist paradigm. An experiment was conducted making use of a mixed methods research design. A mixed methods study can be conducted using an interpretive theoretical lens (Creswell, Shope & Green, 2006; Saunders, Lewis & Thornhill, 2016). The qualitative data was collected through a semi-structured interview with participants, while the quantitative data was collected from Likert Type Scale questions in the questionnaire. The data collection process is illustrated in figure 1.1:

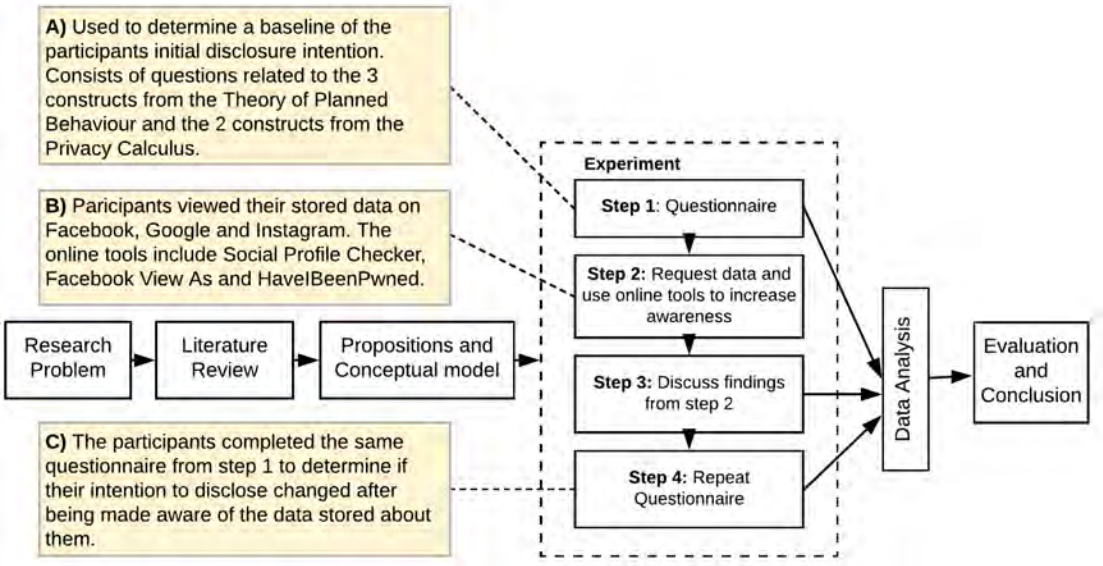


Figure 1.1 Data Collection Process

This 60 to 90-minute experiment was conducted with fourteen students and saturation was reached. To qualify, potential participants must be active Facebook, Google and Instagram users, and be between 18 to 35 years old. This age range was chosen because the most frequent users of Facebook are between 18 and 40 years old (Contena, Loscalzo & Taddei, 2015), while the frequent users of Instagram are between 25 and 34 (Statistica, 2019).

A Thematic Analysis of the qualitative data was conducted using Nvivo 12 to determine important themes within the data based on the constructs in the Theory of Planned Behaviour and the Privacy Calculus. Mind maps were created to visualise each theme in detail, which allowed the researcher to understand the relationships between the emerging concepts. Moreover, the researcher was able to link the perceptions and opinions gathered regarding information disclosure intention and compare these with the quantitative responses from the survey. Finally, descriptive statistics were used to analyse the quantitative data from the survey.

1.7 Ethical Considerations

From an ethical standpoint, researchers should act in a way that prevents loss of data, upholds participant privacy and ensures users provide informed consent (Vannini, 2012). Bearing this in mind, it is imperative that the researcher explains how the participant's information will be used in terms of the study and ensures the participants sign a consent form allowing the use of their information. Furthermore, all participants were informed that participation is entirely voluntary and they are free to opt-out of completing the experiment at any point.

Additionally, all responses from the experiment will remain anonymous and if any sensitive information was discovered about a participant during the experiment, this information was be excluded from the study. Besides responses remaining anonymous, the participants identity will remain confidential. To that end, access to the data collected from the questionnaire will be restricted to only the researcher and supervisor. Finally, ethical clearance was obtained from the Rhodes University Ethics Committee of Human Participants (clearance reference number: 2020-0872-3206) before the experiment was conducted.

1.8 Delimitation of the study

This study focuses on personal information disclosure online, and thus establishing how users manage disclosure in offline contexts is beyond the scope. Furthermore, the study investigates various antecedent factors that influence information disclosure. Regarding these factors, the reader should keep in mind that only a user's personal valuation of their information is examined and therefore, a review of the economic value of personal data is excluded.

Additionally, this study did not examine how personality traits influence the disclosure of personal information online. However, the influence of attitude, subjective norms, and awareness form critical components in understanding information disclosure in this study. Finally, while online privacy is of importance throughout the thesis, the task of this study was not to investigate the extent of the participant's privacy literacy.

1.9 Contribution

This study contributes to a holistic understanding of privacy and information disclosure on social media, specifically among young people in South Africa. Since users do not accurately conduct this cost-benefit analysis (Dhawan, Singh & Goel, 2014; Acquisti, et al., 2015), understanding what influences a user's perception of the benefits and risks related to disclosing online provides new insight into information disclosure. To that end, this study combines the Theory of Planned Behaviour and the Privacy Calculus Theory into a proposed model that can be seen in Figure 1.2. This assists in accounting for the effect social influences have on the cost-benefit analysis users conduct when disclosing information online.

A further contribution to theory is observed in the model where Perceived Behavioural Control is substituted with Awareness. Besides the substitution of this construct, the study also includes the antecedent factors of *Trust in the Social Media Provider*, *FOMO,* and *Personal Valuation of Information* that influence *Attitude*, *Subjective Norms,* and *Awareness*. This is significant, as few studies have investigated the influence of *FOMO* and *Personal Valuation of Information* on intention to disclose personal information, mediated through the Theory of Planned Behaviour. Taken together, the combination of the two theories and antecedent factors provide a unique picture of what encourages and discourages users from disclosing personal information online.

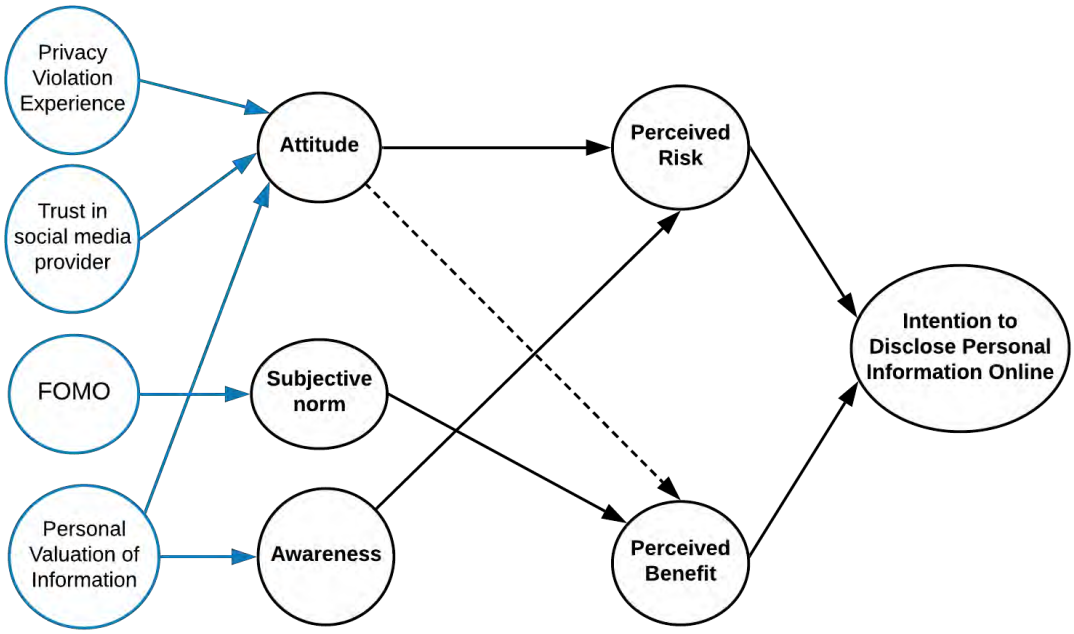


Figure 1.2 Comprehensive Information Disclosure Model

A detailed review of these constructs is provided in Chapter three and four, while Chapter five covers the reasoning behind each proposition.

1.10 Thesis Outline

The overall structure of this study takes the form of nine chapters. The first chapter introduces the study and aims to provide a general overview of the research. Chapter two is pivotal as it discusses the social media landscape and online privacy, with a particular focus on the data collection practices of Google, Facebook and Instagram. Following this, chapter three covers the Privacy Calculus Theory in relation to information disclosure online. This chapter includes a discussion of the constructs in this theory, a review of the factors that

influence these constructs, and the limitations of this theory. Similarly, chapter four discusses the Theory of Planned Behaviour in relation to information disclosure online. Taking this discussion a step further, this chapter also investigates the influence of the antecedent factors *Trust in the Online Platform*, *FOMO,* and *Personal Valuation of Information* on the constructs in the Theory of Planned Behaviour. This leads to chapter five, which provides additional support for the theoretical propositions of this study and concludes with the proposed model.

Chapter six provides a detailed discussion of the research methodology of this study. This includes an overview of the specific context of the participants in this study. Chapter seven analyses the results of questionnaires and interviews undertaken during the experiment. This is followed by chapter eight, where the findings related to each proposition are discussed, and a diagram of privacy decisions is provided. Finally, chapter nine provides a concluding overview of the study with a specific focus on how the research questions were addressed and the contribution this study makes to the field of online privacy.
Figure 1.3 provides a visual illustration of the thesis layout.

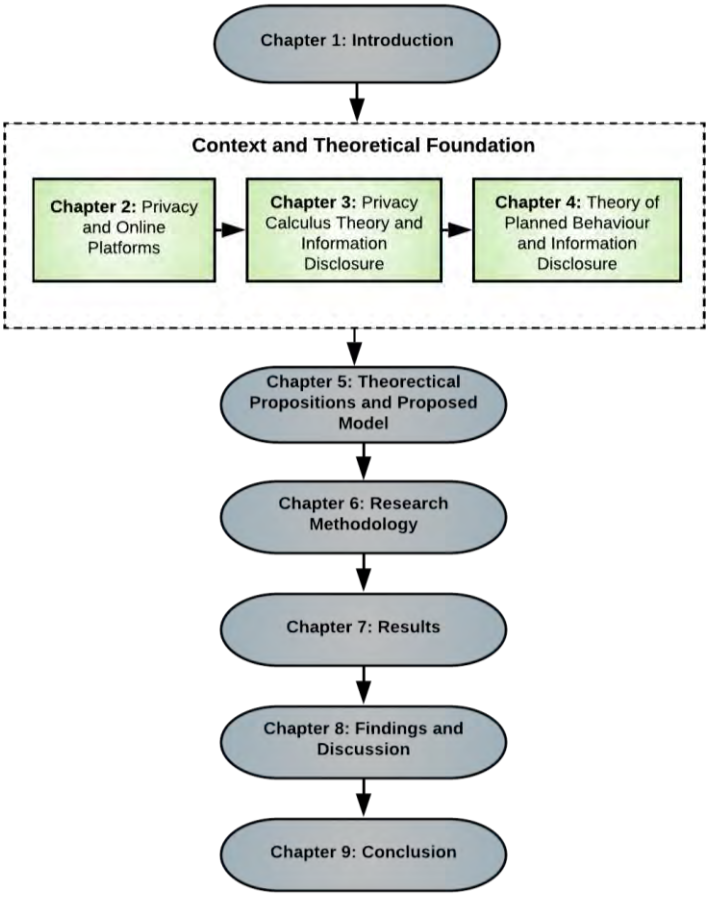


Figure 1.3 Thesis Layout

CHAPTER 2: PRIVACY AND ONLINE PLATFORMS

2.1 Introduction

This chapter aims to provide insight into the nature of data privacy on Google, Facebook, and Instagram. This chapter starts by defining online privacy and discussing the impact of disclosure on determining privacy boundaries. Next, an overview of the General Data Protection Regulation (GDPR) is provided to highlight the potential control users have over the personal data they share online. Following this, an outline of the functioning of Google, Facebook, and Instagram are discussed, and an impression of the social media context is provided. Then, the data practices of Google, Facebook, and Instagram are extracted based on their privacy policies, highlighting the information collected, reasons for collection, and to whom the data is shared. Finally, the resulting findings from analysing these privacy policies leads to a discussion of threats related to sharing information online.

2.2 Conceptualizing Privacy

Understanding privacy in an online context is essential to this study. This includes grasping the influence of the GDPR on a user's ability to access and potentially control the data they disclose.

2.2.1 Online Privacy and Disclosure

Privacy is a complex topic in both online and offline contexts. Westin (1967, p. 337) explains privacy as "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others". In line with this idea, to manage disclosure of information individuals make use of a boundary management process where boundaries represent divisions of public and private information (Petronio, 1991). To regulate the amount of private information a person allows to flow between themselves and other individuals they make use of rules that control these figurative boundaries (Petronio, 1991). In an online context, privacy revolves around regulating the level of access to personal information that defines the self when engaging on online platforms (Trepte, et al., 2015). This includes controlling what information is disclosed both consciously and unconsciously, as well as who can access this information (Alkire, Pohlmann & Barnett, 2019). However, in online contexts, users are willing to

divulge a greater depth of information than they would in offline contexts. This is because online communication lacks the non-verbal and social cues such as eye contact, facial expression and vocal tone that are available in face-to-face communication. (Tsay-Vogel, et al., 2018). In turn, this increased level of disclosure fosters more relaxed privacy boundaries (Tsay-Vogel, et al., 2018).

2.2.2 The GDPR and Control Over Data

Due to issues regarding control over personal data, the General Data Protection Regulation (GDPR) came into effect on 25 May 2018 in Europe (Houser & Voss, 2018). This data protection law is significant to mention because it has impacted the data privacy standards and security measures of online and offline organisations (McGavisk, 2018). The GDPR has three core tenants, the right to portability and access, the right to explanation and the right to erasure (Van Ooijen & Vrabec, 2019). The GDPR states that people should be able to move their data from one organisation to another, thus users should be able to access and download the data stored about them (Heaven, 2018). However, data observed by the platform is not included in the right to access and portability which still poses a threat to user privacy (Van Ooijen & Vrabec, 2019). The GDPR also requires that organisations have to explain, in simple terms, what data they collect, reasons for collection and whether this data is shared with third parties (Matz, Appel & Kosinski, 2020). If the processing of data does not fulfil the requirements of the GDPR the subject of the data has the right to have the data erased (Van Ooijen & Vrabec, 2019). This significantly influences the control users have over the flow of their data when processing is considered unlawful (Van Ooijen & Vrabec, 2019). Thus, the overall aim of the GDPR is to shift some control to users and provides them with a means to control their digital footprint.

2.3 Understanding Google, Facebook, and Instagram

When discussing online disclosure, it is useful to understand the function of each platform in this study as well as the nature of social media.

2.3.1 Overview of Google, Facebook and Instagram

Google is a multifaceted company and Facebook is a social network, but they both aim to help individuals easily find information and communicate (Eadicicco, 2015). Google offers various online services that include a search engine, web browser, email provider, messaging app and many more products (Google, 2020). Google's mission is to organise and make

information useful and accessible on a universal scale (Google, 2020). On the other hand, Facebook and Instagram are all about developing and maintain your online network of friends and followers (Facebook, 2018). To make the most of these platforms they suggest sharing a variety of different information daily (Facebook, 2018). Facebook is based on connecting with friends and user engagement on the platform is driven out of curiosity and the reciprocity of exchanging likes and comments (Serafinelli & Cox, 2019). In slight contrast to this, Instagram is a photo-sharing platform where content is categorised by hashtags and in addition to following friends, users can follow strangers such as celebrities (Serafinelli & Cox, 2019). The common characteristic among all three platforms is the enormous amount of information that they collect about their users.

2.3.2 The Social Media Context

In the digital age engaging on social media has become a prevalent part of daily life, with users of all ages sharing vast amounts of personal information online to foster connections with others (Narayanaswamy & McGrath, 2014). Social media further allows users a variety of communication options that can stir emotions and as such has become a crucial part of many people's daily routines (Cheikh-Ammar & Barki, 2016). The complex nature of social media networks makes it hard for users to be fully aware of their extended network. Users can be connected to various other people and fake profiles through their followers and friends and dependent on their privacy settings the content they post can be viewed by an unknown audience of thousands (Pangrazioand & Selwyn, 2018). To provide some scope of the enormity of information shared on social media sites, every minute on Facebook "510 000 comments are posted, 293 000 statuses are updated, 4 million posts are liked, and 136 000 photos are uploaded" (Osman, 2019). The provision of these large amounts of data can lead to user profiling, as well as targeted communication and advertising when this data is aggregated (Benson, et al., 2015). Since users often skip privacy policies and terms of service notices online, they are unaware of the way their information is collected, stored, processed and shared (Steinfeld, 2016). This leads to information asymmetry, where companies and online platforms have the upper hand due to a greater understanding of their data policies, leaving the user at a loose end (Tesfay, et al., 2018).

2.3.3 Data Practices of These Platforms

To provide a rich contextual background of the online platforms included in this study it is important to highlight what data is gathered and stored about each user, why it is collected and how it is shared.

2.3.3.1 Information Collected

Google collects data on each user over all its applications including YouTube, Google Maps, Gmail and Google Chrome (Williams & Yerby, 2019). The data collected and stored on a user is far more detailed than simply the conscious information volunteered upon creating a profile and also includes unconscious data generation regarding interaction and activity on the platforms. Google collects and stores profile information upon sign-up such as name, gender, birthday, phone number, payment information, emails written and received, photos, documents created and stored on Google Drive, comments on YouTube, contacts and calendar events (Google Data Transparency, 2019). In addition to this, unconscious data is collected in the form of all Google searches performed, all videos watched on YouTube, all ads clicked or viewed, the user's location, devices, apps and browsers used to access Google and all websites visited (Google Data Transparency, 2019). A further break down of the information collected on user activity shows that Google also collects "voice and audio information when you use audio features, purchase activity, people with whom [users] communicate or share content and activity on third-party sites and apps that use [their] services" (Google Privacy Policy, 2019). By logging in on different devices users provide Google with a detailed view of their life and this data can be used to customize content, search results and recommendations without user consent for this personalization (Williams & Yerby, 2019).

To provide a visual summary of the relevant sections of the privacy and data policies of Google, Facebook and Instagram a privacy policy visualization tool was used called Polisis. Polisis uses deep learning, a form of machine learning, to analyse privacy policies and provide a visual representation of, among other things, the data sites collect and share about users (Harkous, et al., 2017). This tool analyses privacy policies by dividing it into small portions that are automatically annotated and labelled to describe the data practices detailed in the policy (Harkous, et al., 2018). Figure 2.1 provides a visualisation, generated by the Polisis Chrome extension, of the data collected by Google. The diagram

highlights the flows of information from the type of information collected on the left to the reason for the collection on the right (Polisis, 2017). Other data in the diagram refers to information that is referred to generically (Polisis, 2017), but in this case refers to information such as data to verify identity and device data for account safety (Google Privacy Policy, 2019).

Facebook and Instagram's data policies also detail the wealth of information collected regarding users conscious and unconscious disclosure. Both platforms have the same data policy that was last revised on 19 April 2018, as Facebook owns Instagram. Similar to Google, these platforms collect information that the user provides as well as usage information. Content provided by the user includes data collected when signing up for the service, messages, shared content, metadata which includes picture location and date of creation and what is seen through the platforms camera feature (Facebook, 2018; Instagram, 2018). Both of these platforms collect information provided about a user through their friends including comments on a user's post by friends, messages to the user from others and when friends upload a user's contact information (Facebook, 2018; Instagram, 2018).

Facebook and Instagram also collect contact information such as the address book, SMS history and call log from uploaded devices (Facebook, 2018; Instagram, 2018). Furthermore, usage information is also collected including content viewed and interacted with on product pages, purchase information such as card number, contact, billing and shipping details and authentication information (Facebook, 2018; Instagram, 2018). Device information such as operating system, device signals, GPS location, photos, cookie data, connection speed etc. is also collected (Facebook, 2018; Instagram, 2018). Finally, data is also stored about a user's interaction outside of Facebook which is sent through Facebook Business Tools from partnering sites (Facebook, 2018; Instagram, 2018). Figure 2.2 on the next page provides a visualisation, generated by the Polisis Chrome extension, of the data collected by Instagram and Facebook. On this diagram, other data refers to facial recognition data, user information provided to vendors and user activity data across Facebook Products (Polisis, 2017).

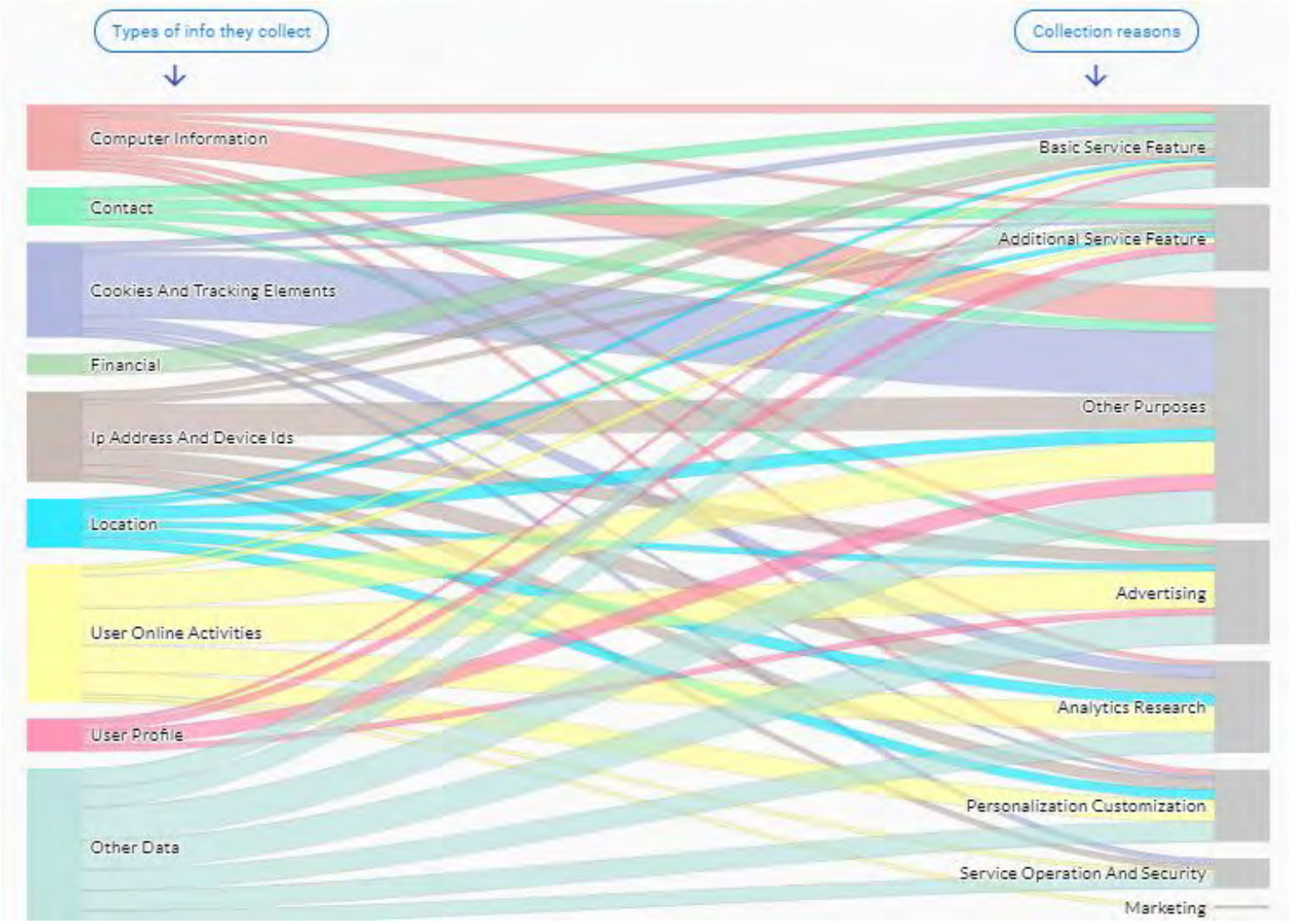


Figure 2.1 Google Data Collection Diagram (Polisis, 2017)

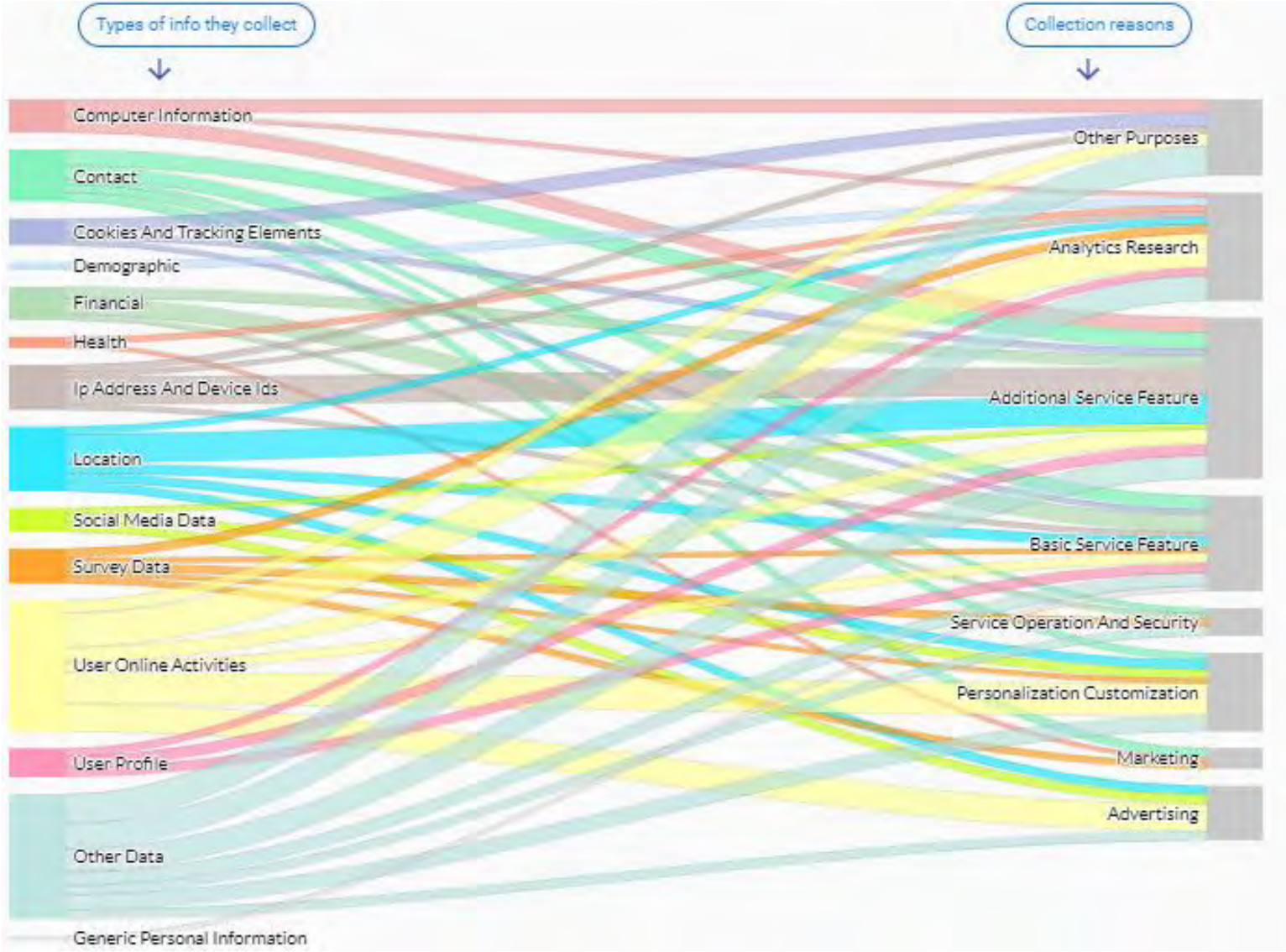


Figure 2.2 Facebook and Instagram Data Collection Diagram (Polisis, 2017)

Overall, it can be seen that Google, Facebook and Instagram collect a significant amount of information on each user. The most concerning thing about the Facebook and Instagram data policy is that not only do these platforms collect data on a user based on the information they upload and their activities, but they also collect information on users through their friends (Bischoff, 2017). Thus, even the most privacy-conscious user can be vulnerable due to their friends with less privacy concerns (Bischoff, 2017)

2.3.4 Reasons for Collecting User Data

Google collects information to provide, maintain, protect and develop its services (Google Privacy Policy, 2019). Figure 2.1 shows the reasons for collection uses for each type of data collected which includes service features, advertising, analytics research, personalization and customization, as well as service operation and security (Polisis, 2017). Google uses data to "understand how services are used", communicate with users, troubleshoot issues and detect, prevent and respond to security risks (Google Privacy Policy, 2019). Furthermore, Google also processes the data collected on users to improve and perfect their algorithms which becomes very valuable when used commercially (Lindh & Nolin, 2016). One of the most significant revenue streams for these platforms is targeted advertising. As such, based on interests Google provides users with personalized ads (Google Privacy Policy, 2019). To determine a user's interests an advertising cookie is stored in their browser to track the content they view online, this information is then used to inferred their demographics and interests to show them adverts they might find appealing (Google, 2020). In terms of revenue creation, Google also includes non-advertising projects such as Google Cloud Platform, Play Store, Chromebooks, Google Apps, Chromecast and Android (Rosenberg, 2018).

Facebook and Instagram use collected data in a similar way, with Figure 2.2 highlighting other purposes with the most data flow (Polisis, 2017). Both platforms use data to personalise content and features such as suggesting groups to join, and products users might find appealing based on site usage (Facebook, 2018; Instagram, 2018). To further personalize products Facebook and Instagram use location information, data from surveys and research for product development, as well as data to enabled facial recognition on content if the user has allowed this function (Facebook, 2018; Instagram, 2018). As with Google, Facebook and Instagram have a targeted advertising system that uses information on user interests to show them personalized advertisements (Facebook, 2018; Instagram,

2018). Users are targeted based on their location, age, gender, languages, education, workplaces and relationship status (Facebook for Business, 2020). Users on Instagram are also targeted based on things they liked in the platform and people they follow, apps and websites visited, as well as their interests and information on Facebook (Instgram, 2020). Other reasons for data collection include analytics and business services, safety and security, research and communication with the user (Facebook, 2018; Instagram, 2018).

2.3.5 Data Sharing Practices

Another important section in any privacy policy refers to how, when and to whom data is shared by the platform in question. Google states that they only share information with companies outside of Google when they have user consent, when an administrator is managing the user's account, for external processing and for legal reasons (Google Privacy Policy, 2019). Non-personally identifiable information might be shared publicly and with partners such as trend reports use of Google services (Google Privacy Policy, 2019). They also allow partners such as YouTube to collect information from a user's browser for advertising using cookies (Google Privacy Policy, 2019). Finally, they highlight that users can manage, review and control data collected and how this data is shared (Google Privacy Policy, 2019).

Facebook and Instagram categorise sharing data in two ways, sharing data on Facebook products/platforms and sharing with third-party partners. These platforms share the content users post to the intended people or accounts based on the user's settings and users can, in turn, see who has viewed their Facebook and Instagram stories (Facebook, 2018; Instagram, 2018). Some of the user's profile information is public based on settings and can be accessed by search engines, API's, apps, websites and offline media (Facebook, 2018; Instagram, 2018). Other people can share information and posts about or from another user, as well as see information about the user's active status on the platform (Facebook, 2018; Instagram, 2018). Websites and third-party apps that use Facebook as authentication have access to information posted or shared, as well as public information on the user's profile (Facebook, 2018; Instagram, 2018). Furthermore, websites with like or share buttons and login via Facebook options put tracking cookies on the user's devices and report behaviour to Facebook to facilitate targeted advertising (Bischoff, 2017). In terms of sharing information with third-parties, Facebook and Instagram share user information with advertisers, vendors and service providers, researchers and academics, as well as law enforcement (Facebook, 2018; Instagram, 2018).

The discussion of the privacy policies of Google, Facebook, and Instagram provides interesting insight into their data practices. In terms of readability, Google's privacy policy is straightforward and easy to follow. Google often makes use of benefit rhetoric, where segments of the policy are framed as something that is done to improve user experience or the service for the user (Lindh & Nolin, 2016). For instance, emphasising that information is collected to deliver better services to users (Google Privacy Policy, 2019), while the commercial value that this data provides to Google is not mentioned. Facebook and Instagram also have an easy to read privacy policy, but it can often be vague and noncommittal (Williams & Yerby, 2019). Additionally, while users believe that they use Google, Facebook and Instagram for free they actually buy these services with their data (Winkler & Zeadally, 2016). As such, storing vast amounts of user data can lead to competitive advantage and powers these tech giants. On the other hand, many users are unaware that their online behaviour and personal information is gathered, stored and shared (Kumar & Nanda, 2019). Furthermore, users also lack awareness regarding the dangers of social media and what can potentially happen to the data they post online (Kumar & Nanda, 2019).

2.3.6 Threats to Personal Information

The disclosure of information by users, as well as the storage and collection practices of platforms, have led to a variety of potential threats to a user's data. Social media platforms are wildly popular and an integral part of daily life because they allow users to stay connected to and share information with friends and family (Rathore, et al., 2017). However, the nature of social media platforms provides cybercriminals with a vast playground of cybercrime to choose from including information leakage, phishing, identity theft, and profiling.

2.3.6.1 Information Leakage

Disclosing information is a requirement for engaging on social media and while this disclosure can facilitate communication it also opens up possibilities for information leakage of a user's identity(Lam, Chen & Chen, 2008). "Information leakage is the phenomena where explicit information provided to a third party can be used to derive implicit and previously hidden information about an entity" (Nouh, et al., 2014, p. 353). The control users have over their data is being progressively lost through each social interaction where private information is leaked (Garcia, 2017). For instance, third-party apps can access personal information through app permissions and can leak this information to Internet

tracking and advertising companies (Chaabane, et al., 2014). The study done by Chaabane, et al. (2014) found 22% of Facebook apps are leaking at least one piece of information, mostly the user ID, to an external entity. Furthermore, Google can track 60% of applications that fall under Facebook (Chaabane, et al., 2014). This poses a serious problem to the privacy of users, as they can be unaware that their personally identifiable information can possibly be leaked when they use these apps. A further example of this privacy leakage is shadow profiles, which refer to profiles on non-users containing private information gathered from the user's contact lists and online browsing behaviour (Garcia, 2017). This means that even if a person does not have a Facebook account, Facebook can still store information about them such as their email address and phone number. These shadow profiles represent the misuse of personal data and on Facebook, they serve as the foundation for the 'people you may know algorithm' (Sujon, 2019). Overall, the dangers of this information leakage are far-reaching and can include phishing, stalking and spamming (Lam, et al., 2008).

2.3.6.2 Phishing

Social media sites are one of the most prominent sources of phishing attacks and involve a cybercriminal posing a trustworthy source to trick users into divulging personal or sensitive information (Silic & Back, 2016). Two stages of attack are employed to facilitate social media phishing. In the first stage the attacker sends a friend request to the victim and after the request is accepted the attacker has access to the victim's information and the other people in their network (Vishwanath, 2015). The second stage of attack involves contacting the user via Facebook messenger to solicit information directly (Vishwanath, 2015). Phishing can lead to serious consequences for users and businesses including a risk to reputation financial loss and loss of sensitive information.

2.3.6.3 Identity Theft

Another increasing threat to social media users is identity theft. Identity theft is a method of attack whereby an attacker copies a user's identity to commit crimes or pursue a target (Kumar & Nanda, 2019). This can be committed in two ways either by hacking and stealing a user's password or by forging a user's account (Kumar & Nanda, 2019). For instance, a cybercriminal steals someone's identity on Facebook and then sends out messages to their Facebook friends asking for money, these concerned friends comply and send money to the criminal (Irshad & Soomro, 2018). Around one-third of users provide at least three pieces

of identifiable information on Facebook that can be used to steal their identity (Irshad & Soomro, 2018). This includes information such as their name, phone number, hometown, pets name, and date of birth (Irshad & Soomro, 2018; Douglas, 2020). Users post this information on Facebook because they trust their Facebook friends (Irshad & Soomro, 2018); however, many of these friends are simply acquaintances that the user does not know well. This is particularly the case on Instagram where around 95 million bots are posing as real users (Ellis, 2019). These bot accounts were originally used to boost the number of followers a user had but their purpose now includes taking over accounts for impersonation scams (Irshad & Soomro, 2018).

2.3.6.4 Profiling

Profiling arises when users are placed into groups based on their gender, race, economic status, and social status (Kumar & Nanda, 2019). Companies collect information about user's behaviour online to create a profile that illuminates their interests and purchasing habits, which is then used to facilitate targeted advertising (Ivana, 2018). User profiles are created by monitoring users behaviour online through tracking cookies in their browser that allow businesses to track advertisement responses, page views and frequency of page visits (Ivana, 2018; Ali, et al., 2017). This profiling can have both positive and negative consequences for users. For instance, profiling on Facebook is used to find friends based on the user's groups and current friends, while Google uses the search history of the user to personalize future search results (Hasan, et al., 2013). On the other hand, these user profiles include personal information about the user and are often sold to third parties to facilitate targeted advertising and can be used for malicious purposes (Hasan, et al., 2013). While platforms such as Google and Facebook attach each profile with a unique identifier and state that they do not sell user information to third parties, by data mining these platforms user data such as name, recent purchases and address can be collected and shared with third parties (Houser & Voss, 2018). Further risks to users resulting from profiling include discrimination, de-individualization, abuse and stereotyping (Schermer, 2013). Taken a step further profiling can lead to psychological targeting where a user's psychological profile is created by analysing a user's digital footprint including their Facebook likes, posts and shares to determine their attitudes, behaviours and emotions (Matz, et al., 2020). For example, in the 2016 US presidential election, Cambridge Analytica extracted millions of Facebook uses psychological profiles to target them with psychologically charged advertising (Matz, et al., 2020). Overall, while profiling can benefit users by personalising

the content they interact with, the act of profiling users raises the issue of whether their privacy is being respected (Hasan, et al., 2013), as all the data they share on social media contributes to their digital profile.

Generally, user awareness of threats to personal information is low, with users not fully understanding the implications of disclosing so much information on social media (Silic & Back, 2016). Users are further limited in their ability to protect their privacy when they are unsure of how platforms use and exploit their information (Barth & De Jong, 2017). Furthermore, without a proper understanding of how to effectively use privacy settings, users are restricted in their ability to control the personal information they share online (Rathore, et al., 2017). Thus, raising user awareness on the data practices of platforms and the privacy settings available to them is paramount when trying to encourage more secure behaviour online.

2.4 Summary

This chapter highlighted the context of data privacy on Google, Facebook and Instagram. In terms of this study, privacy can be thought of as the need to control the flow of private information by instituting boundaries that separate private and public information. Due to the vast amounts of information users share to cultivate intimacy online, privacy boundaries are becoming more relaxed. In addition, by analysing the privacy policies of Google, Facebook and Instagram it can be seen that these platforms collect a significant amount of data on users and could even keep 'shadow profiles' on non-users. Furthermore, even the most privacy-conscious user can be vulnerable due to the information that their friends post about them. Additionally, many users are unaware of what happens to their data once they share it online because they often skip privacy policies. In line with this, users are often unaware of the threats to their data and cybercriminals use this lack of knowledge to their advantage. Therefore, by raising user awareness on the data practices of platforms and the privacy settings users might be more inclined to behave securely online. The next chapter will provide a discussion of previous research on information disclosure and the Privacy Calculus Theory.

CHAPTER 3: THE PRIVACY CALCULUS THEORY AND INFORMATION DISCLOSURE

3.1 Introduction

This chapter aims to provide an in-depth discussion of the Privacy Calculus Theory and information disclosure online. The chapter starts by outlining the Privacy Calculus Theory and investigating its situation-specific nature. Next, the benefit tenet of the Privacy Calculus Theory is discussed, which includes an analysis of the factors increasing a user's perception of benefits related to online disclosure. Then, the influence of risk on information disclosure is outlined by providing an examination of the factors that influence a user's risk perception. Finally, a discussion of the limitations of the Privacy Calculus Theory is presented.

3.2 The Privacy Calculus Theory and Information Disclosure

3.2.1 The Privacy Calculus Theory

The foundation of research related to information disclosure stems from Social Exchange Theory, which states that relationships are based on an assessment of the costs and rewards of social interactions (Homans, 1958). This principle was translated to information disclosure by Laufer and Wolfe (1977), who determined that a person conducts a "calculus of behaviour" to determine whether or not to disclose personal information. The concept proposed that people anticipate the consequences of their current behaviour on the future implications this behaviour might cause. This suggests that people only disclose information when it will be beneficial to them in the long run. However, sometimes individuals feel that the returns for information disclosure override the risk of their privacy being compromised (Dinev and Hart, 2006). Consequently, a loss of privacy is the price one pays for the benefits acquired by disclosing personal information (Hui, et al., 2006). Thus, based on the Privacy Calculus Theory in Figure 3.1, a user weighs the costs against the benefits of disclosure, which affects their intention to disclose personal information.

In this model, benefits increase a user's intention to disclose, while privacy risks decrease a user's intention to disclose personal information (Wirth, Maier & Laumer, 2018).

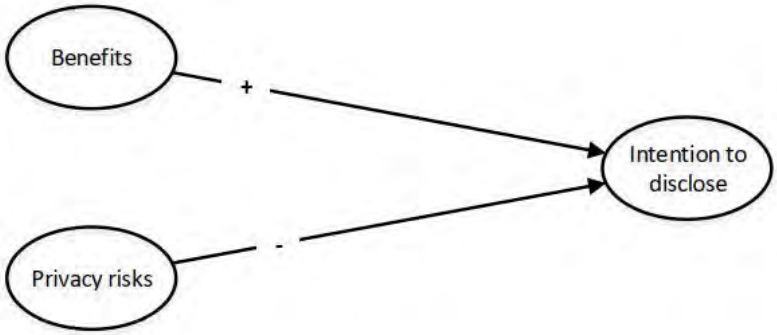


Figure 3.1 Basic Privacy Calculus Model (Wirth, et al., 2018)

In the context of e-commerce, this idea was furthered by Culnan and Armstrong (1999), who argued that consumers would disclose information if the benefits outweighed the risks of that disclosure. They termed this trade-off the "privacy calculus" (Culnan & Armstrong, 1999). While these authors conceptualised this decision-making concept in relation to real-world encounters, Dinev and Hart (2006), applied the Privacy Calculus to the Internet. The study made use of an extended Privacy Calculus Theory that included the additions of privacy concerns and trust to understand factors that predict information disclosure and non-disclosure (Dinev & Hart, 2006).

Following this research, various scholars used the Privacy Calculus Theory to examine information disclosure in the context of social networking sites (Krasnova, et al., 2010; Krasnova & Veltri, 2011; Krasnova, et al., 2012; Min & Kim, 2015; Dienlin & Metzger, 2016). These scholars included various additional factors to the Privacy Calculus Theory to determine information disclosure online. For instance, some studies have investigated the influence of culture on the Privacy Calculus Theory (Krasnova & Veltri, 2011; Krasnova, Veltri & Günther, 2012; Trepte, et al., 2017). A further extended Privacy Calculus Theory was proposed by Dienlin and Metzger (2016), who included the constructs of self-withdrawal and privacy self-efficacy. Self-withdrawal, which refers to withholding information, was predicted by both privacy self-efficacy and privacy concerns (Dienlin & Metzger, 2016). The privacy self-efficacy construct was also used by Chen (2018), to extend the Privacy Calculus Theory and it was found to have both direct and indirect effects on disclosure. Wirth, et al. (2018), included resignation as a construct within the Privacy Calculus and found that with this construct included, the effect of benefits increase, while risks become decreased. In a separate study, the addition of subjective norms was found to be a factor that supersedes both the risks and benefits of disclosure (Wirth, Maier. & Laumer,

2019). The Privacy Calculus Theory has not only been applied to the context of social networking sites. Due to the prevalence of sharing personal health information online, the Privacy Calculus has been applied to virtual health communities (Kordzadeh, Warren, & Seifi, 2016). This theory has also been applied to mobile apps to investigate information (Wang, Duong & Chen, 2016) and continued usage (Zhou & Li, 2014). More recently, the Privacy Calculus Theory has been used to investigate personal information disclosure in the context of IoT services (Kim, et al., 2019). Their study found that users are willing to disclose personal information for personalized services but not for healthcare services (Kim, et al., 2019).

3.2.2 Situation Specific Privacy Calculus

As privacy is dependent on context (Acquisti, et al., 2015), the Privacy Calculus Theory has been argued to be a situation-specific trade-off of perceived risks and benefits. For each privacy decision situation, a user conducts an impulsive, rather than completely logical cost-benefit analysis (Kehr, et al., 2015; Masur, 2018). As a result, it can be assumed that a user's perception of the risks and benefits involved will fluctuate and result in different behaviours based on the specific situation. Thus, factors related to the situation in which the data is being requested might prompt users to perceive disclosure as having increased or decreased risks and benefits (Kehr, et al., 2015). Consequently, decision making is reliant on the context in which the information is being disclosed.

On the other hand, Bol, et al. (2018) highlighted in their study of personalization over the context of news, health, and commercial websites that the Privacy Calculus does not change depending on the context in which it is conducted. Yet, users might have an increased perception of risk when a site calls for the disclosure of sensitive personal information (Bansal, Zahedi & Gefen, 2010). For instance, users might be more willing to share information on social media sites but are far more cautious regarding their privacy on healthcare websites. This might be because, in the context of healthcare websites, users perceive more risks to their personal healthcare data than to the data they post on social media. In line with the original theory of the Privacy Calculus, if the benefits outweigh the risks a user will disclose their personal information. However, the idea of a situational privacy calculus suggests that a user's intention to disclose changes with every disclosure situation and at any time an increased perception of risks or benefits could sway a user to either disclose or not.

3.2.3 Factors Increasing Perception of Benefits

Differing perceptions exist regarding the benefits that ensue following information disclosure online. While limited research has been done on the factors that increase a user's benefit perception (Gómez-Barroso, Feijóo & Martínez-Martínez, 2018), some themes can be identified. These include privacy attitude, perceived control, Internet addiction, social media activity, and privacy awareness.

Privacy experiences form a user's attitude toward disclosing information online. Users who have not experienced privacy violations are more confident online (Gómez-Barroso, et al., 2018) and therefore have a positive attitude towards disclosing information online. These users often perceive more benefits when disclosing information due to their positive attitude. Furthermore, individuals often believe that they are less likely to experience threats to their information compared to other users (Gerber, et al., 2018). Their optimistic bias often attributes risks to others and makes users perceive more benefits related to disclosing information to themselves (Barth & De Jong, 2017). Accordingly, a user's privacy attitude influences their perception of the benefits of social media engagement and information disclosure.

In addition, optimism bias has also been positively related to the perception of control. The higher a user perceives control over their information the more optimistic bias they have in that situation (Cho, et al., 2010). In other words, the more the user believes they have control over the risks to their data, the more they will ascribe risks to others and consider themselves recipients of only the benefits related to information disclosure. Moreover, perceptions of control reduce the fear of privacy violations, which in turn increase a user's perception of the benefits associated with information disclosure online (Hu & Ma, 2010). Many users are knowledgeable about privacy settings but choose not to protect their information because the benefits override the potential threats related to self-disclosure (Barth & De Jong, 2017). Overall, an increased perception of control over information can lead to an increased perception of the benefits related to self-disclosure.

The next factor that increases a user's perception of disclosure benefits on social media is Internet addiction. There has been a debate surrounding whether problematic Internet use can be classified as an addiction or a dependency. Addiction is not restricted to only include substance abuse, as all addictions share various features including "salience, compulsive use (loss of control), mood modification and the alleviation of distress, tolerance and withdrawal,

and the continuation despite negative consequences" (Cash, et al., 2012, p. 292). Internet addiction has many overlapping symptoms with behavioural addictions including mood swings, withdrawal, increased use and a decreased social life (Cash, et al., 2012). Addiction to the Internet can occur due to depression, loneliness and stress (Xu & Tan, 2012) and can cause, among other symptoms, an increased risk tolerance (Guedes, et al., 2016a). Users who are addicted to the Internet and social media perceive more benefits related to information disclosure online (Gómez-Barroso, et al., 2018), as these sites provide users with the opportunity to fulfil their need to belong and give them the opportunity for self-presentation (Guedes, et al., 2016a). Furthermore, people have an inherent desire to self-disclose in order to foster relationships, this disclosure is mandatory in social networks and activates the brain's reward centre (Guedes, et al., 2016a; Guedes, et al., 2016b). Sharing information about oneself online can be a rewarding experience, similar to the experiences people receive from "primary rewards such as food and sex" (Tamir & Mitchell, 2012). When a user is addicted to the Internet, they excessively use social media and become dependent on the satisfaction they gain from self-exposure, which gives them an increased perception of the benefits related to information disclosure (Guedes, et al., 2016a).

Besides Internet addiction, increased online activity also leads to a heightened perception of the benefits related to information disclosure (Gómez-Barroso, et al., 2018). This online activity includes online shopping, banking, gaming, blogging, watching videos and social media usage that heightens the user's perception of the convenience of the Internet. For example, users of a platform are far more likely to perceive increased benefits related to information disclosure than non-users. Steijn, Schouten and Vedder (2016) concluded that in comparison to non-users of Facebook, users believe benefits are more likely to occur than privacy risks. Thus, the use of online platforms increases a user's benefits perception.

Additionally, users will disclose more if they receive feedback in the form of comments and likes, which simulate the reward centres in the brain (Guedes, et al., 2016a). Thus, despite the risks, individuals who spend more time online will frequently post and use social media to receive the perceived benefits of self-presentation and belonging. Furthermore, posting, and sharing online is a habit that promotes a sense of connectedness and creates social capital, which in turn make these benefits seem far more immediate than the potential risks (Debatin, et al., 2009).

The final factor that increases a users benefit perception is their privacy knowledge and awareness (Gómez-Barroso, et al., 2018). A lack of awareness regarding the significance of personal data and the potential threats to this data result in users perceiving maximum benefits and little risk (Barth & De Jong, 2017). Many users continue to voluntarily disclose personal information and do not engage in secure online behaviour (Shillair, et al., 2015). This might be due to a lack of knowledge surrounding strategies to prevent vulnerabilities and alleviate threats online (Junger, Montoya & Overink, 2017). Consequently, less privacy awareness and knowledge result in users making disclosure decisions centred around incomplete information, which can lead to irrational privacy decisions based on an overestimation of the benefits involved (Gerber, et al., 2018).

Figure 3.2 below provides an illustration of the identified factors that increase a user's perception of the benefits related to disclosing information online.

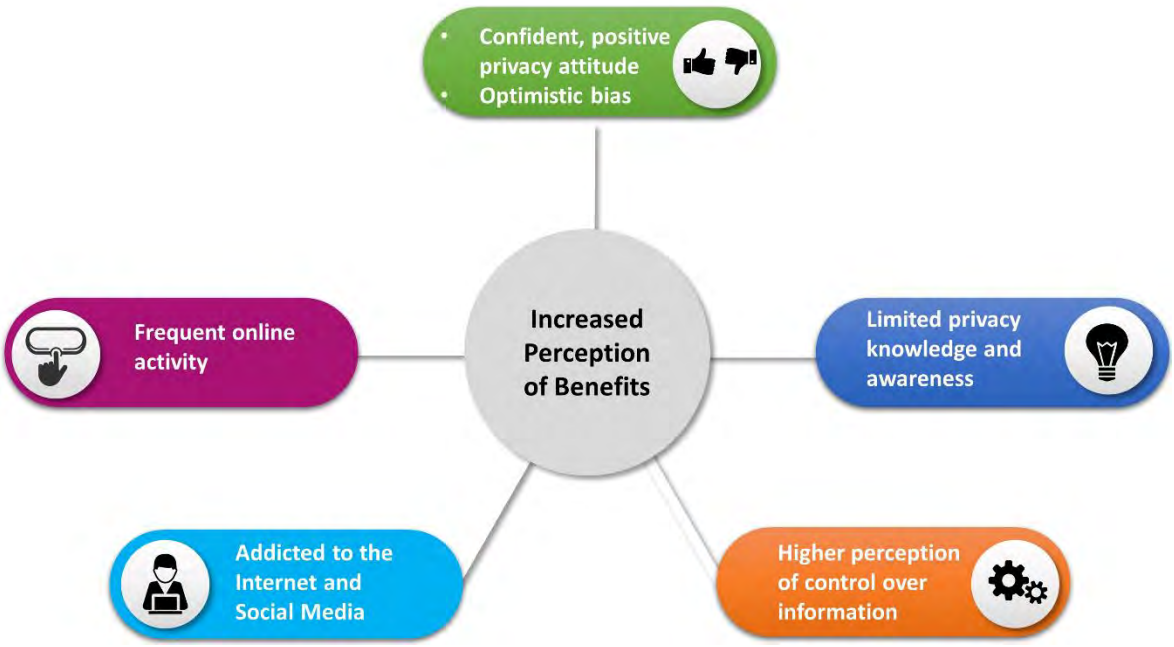


Figure 3.2 Factors Contributing to an Increased Perception of Benefit

3.2.4 The Influence of Perceived Benefits on Information Disclosure

The most significant reason why users disclose personal information social networking sites are the expected benefits (Krasnova, et al., 2010; Gerber, et al., 2018). Disclosing information can be inherently rewarding (Abramova, et al., 2017) and the benefits of self-disclosure have been found to positively influence information disclosure across various contexts on the Internet. The most prevalent benefit of self-disclosure on social media is relationship management (Krasnova, et al., 2010; Krasnova & Veltri, 2010; Min & Kim, 2015; Abramova, et al., 2017; Vishwanath, Xu & Ngoh, 2018; Heravi, Mubarak. & Choo, 2018), which includes maintaining new and existing relationships, reciprocal information sharing and increasing social capital. By using social networking sites, users can conveniently maintain relationships, which in turn, generate social capital and a sense of connectedness (Koroleva, et al., 2011). The convenience to keep in contact with their friends has also been noted as a benefit of using and disclosing information on social media platforms (Krasnova & Veltri, 2010).

Furthermore, enjoyment is also an important benefit of self-disclosure online (Krasnova & Veltri, 2010; Krasnova, et al., 2012; Heravi, et al., 2018). The entertainment that users derive from sharing posts and pictures, watching videos, and playing games urge the disclosure of personal information and participation on social media platforms (Krasnova, et al., 2010). Social networks also allow users to effectively control their self-presentation, which has a considerable effect on their intention to disclose personal information (Min & Kim, 2015). Thus, people engage on social networks to shape an appealing self-image to their online friends (Marwick & Boyd, 2011). In order to successfully create this image, users share vast amounts of personal information, which increases their susceptibility to privacy threats (Koroleva, et al., 2011). Additionally, different social media sites can be used to attain specific benefits. For instance, Instagram can foster social interaction and self-expression, while Facebook provides a space for self-presentation and belonging (Kircaburun, et al., 2018).

Benefits have been found to override privacy risks and concerns when actively engaging on social media. For instance, even when users have experienced an invasion of privacy the benefits of using Facebook have still been found to overshadow privacy concerns (Debatin, et al., 2009). Moreover, Min and Kim (2015) found that the benefits of social networking cause users to disclose information. In their determination of the antecedents of information

disclosure on social networking sites, Li et al. (2016), found perceived benefits to increase a user's willingness to self-disclose information. Similarly, Dienlin and Metzger (2016) concluded that perceived benefits significantly predict self-disclosure on social networking sites. Consequently, the immediate benefits of disclosure outweigh the potential future risks to a user's privacy (Acquisti, et al., 2015). Yet, some scholars have found benefits to have little influence on self-disclosure intentions and behaviours (Han, et al., 2019). In a qualitative study of self-disclosure on social networking sites, it was unclear whether the benefits of self-disclosure outweigh the risks (Heravi, et al., 2017). Only one participant admitted to favouring benefits over risks, thus perceived benefits did not have a significant impact on self-disclosure intention (Heravi, et al., 2017). Thus, no evidence was found to confirm that users apply the Privacy Calculus Theory in the context of social networking, as many of their participants felt neither risks nor benefits had any bearing on their decision to disclose online (Heravi, et al., 2017). Additionally, in a study investigating the management of privacy on Facebook, users focused on the benefit of social need fulfilment over the risks associated with lax privacy settings (Vishwanath, et al., 2018). These researchers also found that in relation to privacy management cost and benefits are juxtaposed against one another (Vishwanath, et al., 2018).

The influence of benefits on self-disclosure are also evident in other communication avenues on the Internet. For instance, benefits have had a considerable influence on self-disclosure in the context of personal blogging. Stefanone and Jang (2007) concluded that the benefits of communicating via blogging overshadow the perceived cost of relinquishing control over one's personal information. Investigating micro-blogging in China, Liu, et al. (2016) found that when users perceived opportunities to develop relationships and derive enjoyment from their blogging activities, they are positively influenced to disclose information. Furthermore, in e-commerce, users disclose to gain tangible rewards such as coupons, discounts and personalized services (Jiang, Heng, & Choi, 2013). In this context, the most noteworthy reason for information disclosure is personalization (Zhao, Lu & Gupta, 2012). Examining how personalization influenced self-disclosure over the contexts of health, commercial and news websites Bol, et al., (2018) found perceived benefits to be the strongest predictor of a user's willingness to self-disclose information online. Bol, et al., (2018), also noted that sometimes monetary rewards limit users' willingness to disclose information because the information requested by the site has little to moderate relevance. Interestingly, benefits

were found to have no impact on a user's willingness to disclose personal information for personalised recommendations on YouTube (Kim & Kim, 2018).

Overall, these studies point to the significant role perceived benefits play when it comes to information disclosure intention and behaviour online. While benefits differ over the many contexts of the Internet, a user's perceived benefits have been seen to positively influence information disclosure online. Thus, if a user anticipates increased benefits, they are more inclined to disclose personal information to reap the rewards this disclosure could offer.

3.2.5 Factors that Influence Risk Perception

An individual's perception of risk is influenced by various factors that motivate their privacy-protective behaviours. The first factor that can be identified is attitude, which significantly influences a user's perception of risk. Van Schaik, et al., (2018) determined that attitude is a significant predictor of risk perception. A user will have an increased perception of risk if they have experienced a privacy violation (Gerber, et al., 2018). Following the privacy invasion, the user will have a more concerned attitude towards disclosing information and will be more inclined to anticipate potential risks to their privacy. An attitude that leads to behaviour is formed by personal experiences, thus negative information disclosure experiences will lead to an increased perception of risk and ultimately a lower intention to disclose information (Dienlin & Trepte, 2015). Furthermore, a positive attitude towards the platform translates to a lower perception of risk. Van Schaik, et al. (2018), found that users with a positive attitude towards Facebook and its privacy settings perceived less risk to their online privacy when engaging on the platform. Additionally, if a user feels a responsibility to protect their data they will have a more concerned attitude, which will lead to an increased perception of risk (Gerber, et al., 2018; Millham & Atkin, 2018). As with a user's perception of benefits, optimism bias plays a role in the perception of risks. Users often avoid using tools to protect their privacy due to optimism bias (Weinberger, Bouhnik & Zhitomirsky-Geffet, 2017). Thus, optimism bias might cause users to have a lower perception of the risks to their personal data because they believe privacy violations are more likely to happen to others.

Another factor that affects a user's perception of risk is awareness. Users have a higher risk perception if they are aware of general privacy risks (Gerber, et al., 2018). For example, extreme privacy-related events such as the Cambridge Analytica breach increases a user's privacy awareness, which increases their perception of potential risks to their data (Van

Schaik, et al., 2018). At the same time, a lack of awareness could lead to user not accurately perceiving the risks to disclosing information online. Users also voluntarily disclose personal information on social media due to a lack of awareness regarding the threats (Weinberger, et al., 2017). As a result, they do not protect their personal data enough to ensure its safety (Dhawan, et al., 2014). Additionally, Zlatolas, et al (2015), determined that awareness increases privacy concern. Thus, knowledge of privacy makes users concerned about the information they disclose (Zlatolas, et al., 2015).

The next factor influencing risk perception is social norms related to online privacy and information disclosure. Social influence affects a user's privacy decisions, with users feeling obligated to reciprocate the level self-disclosure of their peers (Gerber, et al., 2018). This is because users can easily see what their friends and followers share, post, like and do, which might make them feel pressured to disclose more personal information (Cheung, et al., 2015). Social norms influence an individual's perception of risk, as their peer network's attitudes and behaviours toward risk affect their risk behaviours and attitudes (Geber, et al., 2019). Moreover, the perception of social norms determines how willingly users will carry out certain behaviours (Shillair, et al., 2015). For instance, if a user feels it is a social norm for them to be privacy-conscious and protect their personal information, they will have an increased perception of the risk to their data and be more inclined to follow privacy-protective behaviours to protect their personal information. On the other hand, if they feel it is a social norm to disclose vast amounts of personal information, they might have a decreased perception of the risks related to their data and not follow privacy-protective behaviours. Thus, social norms can either strengthen or weaken a user's perception of risks, which in turn influences their willingness to disclose personal information online.

Finally, demographic factors have been seen to influence a user's perception of privacy risks and concerns. When making privacy decisions woman focus more on risks whereas men focus on benefit (Sun, et al., 2015). This is because women have been found to be more concerned about threats to the privacy of their information by Facebook, third-parties and other users (Fogel & Nehmad, 2009; Farinosi & Taipale, 2018). This finding is supported by Hoy and Milne (2010), although they determined that overall women remain ambivalent regarding privacy. Interestingly, women tend to disclose more in-depth online even although they are inclined to be more concerned regarding the privacy of their information (Gerber, et al., 2018). On the other hand, men have been found to perceive less risk (Gerber, et al.,

2018). In a study investigating the contact information people disclose on social media, men were more prone to reveal their address and phone number (Taraszow, et al., 2010). Conversely, some scholars have determined that gender differences do not significantly influence a user's privacy concerns (Hazari & Brown, 2013; Dhawan, et al., 2014).

Additionally, privacy concerns have been seen to heighten with age. Some studies have found that younger adults are often less concerned about privacy (Benamati, Ozdemir & Smith, 2017; Gerber, et al., 2018). Kezer et al, (2016) determined that older adults are less inclined to use privacy protection and tend to disclose less personal information online. Similarly, Steijn, et al. (2016), found that older people have more privacy concerns and connect privacy with situations that require personal data. This might be because users between the age of 18 and 22 remain unaware of the threats related to disclosing accurate personal data, such as phone numbers and home addresses (Taraszow, et al., 2010). Nevertheless, Dhawan, et al. (2014), found young adults between 21 and 40 to be more concerned regarding the privacy of their data compared to teens and older adults. Additionally, Taddicken (2014) found age to have no influence on privacy concerns. Users between the age of 18 and 22 are unaware of the threats related to disclosing accurate personal data, such as phone numbers and home addresses (Taraszow, et al., 2010). Accordingly, both age and gender play a role in a user's perception of privacy risks and concerns.

Figure 3.3 below provides an illustration of the factors that influence a user's perception of the risks related to disclosing information online.

Figure 3.3 Factors Influencing Perception of Risk

3.2.6 The Influence of Perceived Risks on Information Disclosure

The Privacy Calculus Theory also states that costs of information disclosure influence behaviour. These costs refer to the perceived consequences of self-disclosure that deter users from sharing information on social media (Abramova, et al., 2017). Research on the Privacy Calculus thus far have either used privacy concerns or perceived privacy risk to determine the costs of disclosure (Krasnova, et al., 2009; Krasnova, et al., 2010; Lowry, Cao & Everard, 2011; Dienlin & Metzger, 2016; Weinberger, et al., 2017). Perceived risks refer to the harmful consequences of sharing personal information (Chang, et al., 2017), while privacy concerns refer to the extent to which an online user is concerned about the collection, storage and use of their personal information (Koohang, Paliszkiewicz & Goluchowski, 2018). Both of these concepts highlight the anxiety related to potentially experiencing a loss due to disclosing personal information online (Dienlin & Metzger, 2016).

Digital traces of personally identifiable information stored by online platforms pose a severe threat to a user's privacy (Vishwanath, et al., 2018). By linking third-party apps with accounts such as Google and Facebook users are disclosing data in an even greater manner, which allow attackers a single point of access to their identity. This increased integration of social media with third-party apps provides increased opportunities for online crime. Moreover, users often underestimate the risks of disclosing personal information when they are confronted with the benefits disclosure can offer (Kehr, et al., 2015). For instance, in order to increase popularity and a sense of belonging individuals will often accept friend requests from acquaintances and possibly strangers. The addition of these virtual strangers to the user's friend network poses risks to the privacy of their data (Choi, et al., 2018). These risks to a user's personal information on social media include cyberbullying, profiling, scams and surveillance (Nyoni & Velempini, 2018). Additionally, extensive disclosure can also lead to exposure to risks that could endanger the user's safety. For example, posting location data while on holiday could lead to a user being burgled (Nyoni & Velempini, 2018).

Furthermore, when engaging on social media sites users place far more importance on perceived benefits, however, on e-commerce websites, behaviour tends to be determined more by perceived risk when deciding whether to disclose their personal information (Loiacono, 2015). Nevertheless, perceived privacy risks and concerns often decrease self-disclosure on social media. Testing the interaction between privacy risks and perceived benefits in location-based social networks, (Sun, et al., 2015) determined that privacy risks

reduce the relationship between benefits and intention to disclose information. While effects of perceived risks on information disclosure online are lower than perceived benefits, risks still have a significant negative influence on the amount of information a user is willing to disclose (Krasnova, et al., 2010). However, Steijn, et al. (2016) suggests individuals believe it is more likely to reap the benefits from engaging and sharing personal information on social media than for privacy risks to occur. This might be due to user's often attributing increased privacy risks to other people and fewer risks to themselves, which increases the likelihood that perceived benefits will overshadow the risks of disclosing information (Debatin, et al., 2009). As such, until the risks of posting personal information online are felt personally by the user, they believe they are immune to these threats.

In line with this idea, studies have found that perceived benefits outweigh privacy concerns (Zhao, et al., 2012; Dienlin & Metzger, 2016), although privacy concerns prevent individuals from disclosing information on social media (Min & Kim, 2015). A high perception of risk will outweigh the benefits a user might gain, thus limiting information disclosure. Consequently, perceived risk has a significant negative effect on self-disclosure (Kroll & Stieglitz, 2019). Moreover, the significance privacy concerns have in reducing disclosure is determined by whether a user is risk-averse or risk-tolerant (Krasnova, et al., 2012). Krasnova, et al. (2012), examined the effect of culture on information disclosure and found that privacy concerns affected the risk-averse German users more than the risk-tolerant US users.

Privacy concerns have also been seen to encourage users to restrict the visibility of their profile on social media, however, this caused users to disclose more information and increase their friend network (Chen, 2018). Interestingly, Heravi, et al. (2017) determined that perceived risk has a far greater effect on whether users choose to disclose their personal information on social media. Thus, users will behave in a more cautious manner when they want to prevent the risks associated with social media engagement from occurring (Trepte, et al., 2017). A user's perception of risks also has an effect on their overall attitude towards disclosure. Thus, a higher perception of the risk to the privacy of their data will foster a negative attitude towards disclosing information and vice versa. On the other hand, some studies found that perceived risks and privacy concerns have no significant effect on information disclosure (Taddicken, 2014; Cheung, et al., 2015).

In other spheres of the Internet, privacy risks and concerns also play a role in the decision to disclose information. Perceived privacy risks reduce a user's self-disclosure when blogging (Liu, et al., 2016). These risks determine the level of information a user is willing to disclose, as revealing information that can identify the blogger poses a threat to their privacy and potentially their safety (Stefanone & Jang, 2007). In the context of e-commerce, perceived risk has also been seen to limit information disclosure. For instance, privacy concerns have been found to impede transactions on e-commerce websites (Dinev & Hart, 2006). Additionally, perceived privacy risk decreases the likelihood that a user is willing to disclose their personal information in health, news and e-commerce contexts (Bol, et al., 2018). Thus, users who believe the privacy of their information is more at risk are somewhat less inclined to disclose (Bol, et al., 2018).

The findings from these authors reveal the lack of consensus regarding the extent to which perceived risks influence a user's intention to disclosure. Privacy risks discourage user's from disclosing information online. However, these risks still have a lower impact on actual disclosure than perceived benefits. This calls for further investigation into the factors that influence a user's perception of privacy risk and how these perceptions influence their intention to disclose information.

3.2.7 Limitations of the Privacy Calculus

A limitation of the Privacy Calculus Theory is that it assumes privacy-related decisions are made rationally. However, information disclosure online is often context-dependent, automatic and emotionally influenced (Masur, 2018). Furthering this idea, some studies have shown that it is seldom that users approach decision making in a calculative manner (Wilson & Valacich, 2012). A reason for this could be that users do not accurately conduct this cost-benefit analysis due to misguided risk perceptions (Dhawan, et al., 2014; Acquisti, et al., 2015). In other words, when users are conducting this cost-benefit analysis they believe the risks to be lower than the benefits when it is actually in reverse. This is because individuals lack the ability and relevant information needed to accurately assess the risks and benefits related to disclosing (Kokolakis, 2017). Yet, some studies have found that neither perceived risks nor perceived benefits influenced self-disclosure on social networking sites, which suggest the Privacy Calculus Theory alone might not fully explain disclosure intention (Dhawan, et al., 2014).

This points to the notion that privacy decisions are a lot more complicated than first anticipated. Rather than simply being a rational evaluation, various personal factors influence information disclosure intention (Knijnenburg, et al., 2017). Dienlin and Metzger (2016), suggest it would be constructive to integrate a "socially oriented theory" such as the Theory of Planned Behaviour with the Privacy Calculus to examine social influences. Furthermore, while costs and benefits significantly affect the likelihood of disclosure occurring, it does not determine the disclosure of personal information (Dienlin & Trepte, 2015). Therefore, this study suggests integrating factors from the Theory of Planned Behaviour such as privacy attitude, subjective norms and awareness with the Privacy Calculus to better understand the potential cost-benefit analysis a user conducts when disclosing information.

3.3 Summary

This chapter discussed Privacy Calculus Theory in relation to information disclosure on social media. Benefits were found to be one of the main predictors and motivators of self-disclosure on social media. As such, benefits often override privacy risks and concerns when actively engaging on social media. While perceived privacy risks discourage a user from disclosing information online there is a lack of consensus regarding the extent of this discouragement. Privacy decisions are a lot more complicated than first anticipated thus this study proposes the integration of the Theory of Planned Behaviour with the Privacy Calculus Theory. Thus, the next chapter will discuss the constructs from the Theory of Planned Behaviour in relation to information disclosure online.

CHAPTER 4: THE THEORY OF PLANNED BEHAVIOUR AND INFORMATION DISCLOSURE

4.1 Introduction

In this chapter, the constructs within the Theory of Planned Behaviour are examined in relation to information disclosure online. The chapter begins by providing a general overview of the Theory of Planned Behaviour. Next, each construct that leads to intention is discussed in relation to online information disclosure. Finally, the chapter concludes by providing an argument for the replacement of perceived behavioural control with awareness.

4.2 Theory of Planned Behaviour and Information Disclosure

4.2.1 Theory of Planned Behaviour

In online situations users cannot depend on their physical senses to identify risks to their privacy, thus effective protection of personal information and privacy online involves plenty of thought and deliberate actions (Yao, 2011). As no single factor can be used to explain behaviour, it is useful to apply a theoretical framework that attempts to understand what drives an individual's intention to engage in a specific behaviour. Therefore, a combination of the Privacy Calculus Theory and the Theory of Planned Behaviour will be used as the theoretical foundation of this study.

Due to the limitations of the Theory of Reasoned Action, an extended version of the theory was created called the Theory of Planned Behaviour (Ajzen, 1991). Both theories are used to predict a person's intention to engage in a specific behaviour. However, the addition of the construct perceived behavioural control allowed the Theory of Planned Behaviour to account for behaviours where individuals have the ability to exercise self-control (Roberts, 2012). Consequently, this theory has become one of the most popular and significant theories for research into human action (Ajzen, 2002). The theory posits that behavioural intention is determined by an individual's attitude towards the behaviour, subjective norms and perceived behavioural control (Ajzen, 1991). Following this, the theory also proposes that intention leads to actual behaviour, thus intention is an immediate precursor of actual behaviour (Ajzen, 2002). Figure 4.1 provides a diagram of the Theory of Planned Behaviour.

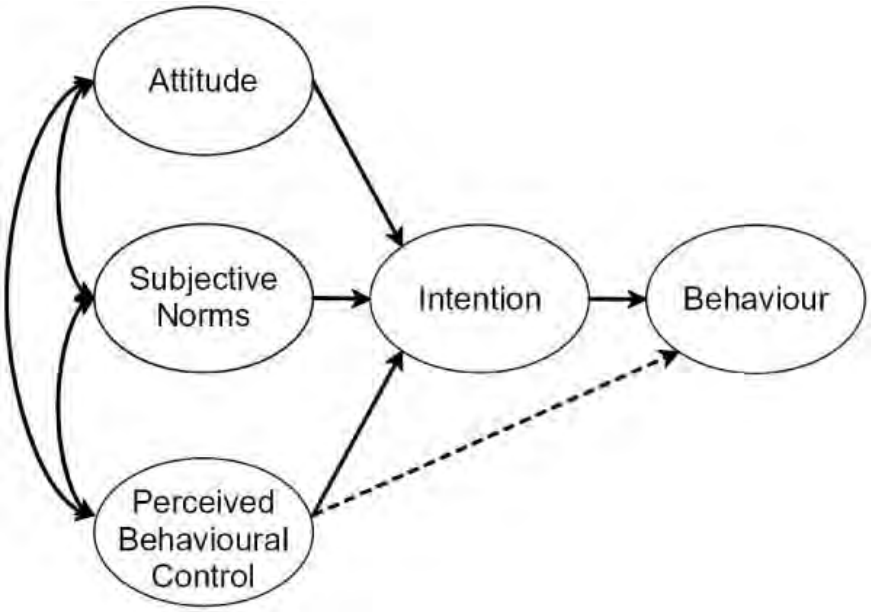


Figure 4.1 Theory of Planned Behaviour (Ajzen, 1991)

The five constructs in the model can be described as follows:

i. Attitude refers to whether a person considers performing the behaviour as either positive or negative (Ajzen, 1991). A person's attitude is based on their beliefs and involves contemplating whether the behaviour will have the desired outcome.
ii. Subjective norm is defined as a person's perception of the social pressure related to performing the behaviour or not (Ajzen, 1991).
iii. Perceived behavioural control refers to the level of difficulty involved in performing the behaviour (Ajzen, 1991)
iv. Intention is the central construct of this theory and refers to how motivated a person is to execute a specific behaviour (Ajzen, 1991).
v. Behaviour refers to whether a person acts in the situation and is informed by behavioural intention together with perceived behavioural control (Ajzen, 1991).

As attitude is derived from the beliefs a user has about the behaviour, if a user has a positive attitude towards sharing information, they will be more likely to self-disclose online. Subjective norms are a product of beliefs surrounding whether performing the behaviour is expected or not expected by important peers. Thus, if a user believes they should be sharing personal information online to reciprocate the level of disclosure provided by their peers,

they will have an increased intention to disclose personal information. Following this, their perceived behavioural control will influence their perception of how likely they are to successfully perform the behaviour. As such, if the user believes they are able to disclose information online because they have the ability and resources necessary, they will have an increased intention to perform this behaviour. Overall, that the more positive the subjective norms and attitude are, the more control a user will perceive and the stronger their intention to execute the behaviour will be (Ajzen, 1991). The importance of these constructs varies across different behaviours and situations, therefore, in one situation attitudes alone might account for intention, while in another situation all three constructs might account for intention (Ajzen, 1991).

While the Theory of Planned Behaviour has been used extensively to predict health-related behaviours, due to its generalizability it can be applied to various other behaviours (Godin & Kok, 1996). As such, this theory has also been used to determine several online security behaviours. For instance, the Theory of Planned Behaviour has been used to determine the willingness to disclose personal information by adolescents on commercial websites (Heirman, et al., 2013). This study proposed an extended Theory of Planned Behaviour, with additional antecedents influencing attitude and perceived behavioural control. Moreover, the results indicated that social factors override attitude, as teens are highly influenced by peer pressure (Heirman, et al., 2013). Similarly, in a study on cybercrime, Burns and Roberts (2013) used the Theory of Planned Behaviour to predict online protective behaviour and found a strong relationship between subjective norms and intention to engage in online protective behaviour or not. Investigating the beliefs influencing a user's attitude and intention to use Facebook privacy controls, Taneja, et al., (2014) concluded that intention to use these controls is determined by social norms and attitude, which is further determined by the benefits and costs of use. Additionally, Kim, et al. (2016) applied this theory to selfie posting behaviour and determined that attitude, subjective norm, narcissism and perceived behavioural control are all contributing factors to a user's intention to post selfies online.

Besides these studies, Yao (2011) states that the Theory of Planned Behaviour would be useful in examining online privacy management because privacy protection behaviours are similar to various health-related behaviours. Self-disclosure involves a calculated decision of whether to perform the behaviour based on individual and contextual influences. Thus,

this theory combined with the Privacy Calculus would provide a more comprehensive evaluation of a user's intention to disclose personal information online (Xu, et al., 2013). The main aim of the Theory of Planned Behaviour is to supply a dependable model that correctly explains human behaviour and predicts both intention and actual execution of various human behaviours (Ajzen, 1991). The original model does not account for antecedents to attitudes, subjective norm and perceived behavioural control. However, to effectively understand information disclosure the factors that influence a user's privacy attitude, subjective norms and awareness need to be explored. The remainder of this chapter will discuss these constructs and identify the antecedents that could be included in this study.

4.2.2 Privacy Attitude and Information Disclosure

Attitude is a central factor in determining a user's privacy beliefs and behaviour. Studies investigating online interactions often use privacy attitude and privacy concerns interchangeably. However, while these concepts are essentially related, they are different (Kokolakis, 2017). Privacy attitude refers to a general assessment of various privacy-related behaviours as either bearing a positive or negative consequence (Gerber, et al., 2018). Whereas privacy attitudes are related to specific behaviours, often privacy concerns are not determined by context and can be rather generic (Kokolakis, 2017). Furthermore, while privacy attitudes can be either positive or negative and are thus bipolar, privacy concerns are unipolar and only measure if the user has a negative view of disclosure (Dienlin & Trepte, 2015). Consequently, attitude is a far more adaptable construct, that can be applied to various situations. Moreover, the study found that privacy concerns can influence attitude since users who had evident privacy concerns were more suspicious and unsure of posting personal information online (Dienlin & Trepte, 2015).

Additionally, attitudes are generally researched using two components, namely, affective attitudes and cognitive attitudes (Dienlin & Trepte, 2015). The affective aspect of attitude refers to the feelings and emotions associated with a behaviour, while the cognitive aspect involves an individual's thoughts and rational reactions (Debatin, et al., 2009; Padyab, et al., 2019). Examining the potential cost-benefit analysis users conduct is often used to provide insight into the cognitive aspect of attitude (Padyab, et al., 2016). It can also be noted that when users have limited awareness of the dangers to their data, affective attitudes have a larger impact on their decisions (Padyab, et al., 2019). Once a user's attitude moves from affective response to negative cognitive reaction, they are more inclined to protect their

information. In the study of the online disclosure of online shoppers, Li, et al. (2017) determined that the cognitive reactions users form during their first interactions with a website is a prevailing predictor of privacy-related behaviour. Thus, if a user has a positive cognitive reaction, they would be more inclined to disclose their personal information online (Li, et al., 2017).

Privacy attitudes have been shown to significantly influence information disclosure intention. A user's general attitude towards privacy significantly influences their disclosure behaviour (Stutzman, Capra & Thompson, 2011). Accordingly, a negative privacy attitude decreases the probability that a user will disclose their personal information and vice versa. Interstingly, Joinson, et al. (2010) determined that both general privacy attitude and situation-specific attitude predicts a users privacy behaviour. Thus, a user's evaluation of both the disclosure behaviour and the situation in which the personal information is requested determines whether their willingness to disclose their information.

Furthermore, a study conducted in the corporate environment found that attitude plays a significant role in security policy compliance intention, which suggests that an individual's attitude towards compliance is vital in influencing positive intentions (Ifinedo, 2012). In a study examining the causes of personal information protection intention, Chon, et al. (2018) concluded that attitude has a positive influence on a user's intention to protect their personal information on Facebook. They suggest that improving a users attitude towards protecting their information online can prevent the leakage of their personal information on platforms such as Facebook (Chon, et al., 2018). Dienlin and Trepte (2015) differentiated between social, psychological and informational privacy attitudes and found that these attitudes had a positive indirect effect on a user's intention to disclose and a direct positive effect on behaviour. Users who believe concealing their identity online is a good idea have an increased intention to conceal their information and will attempt to behave in a way that facilitates this concealment (Dienlin & Trepte, 2015). Whereas users with more relaxed opinions regarding privacy have a greater intention to disclose personal information online (Tsay-Vogel, et al., 2018). A cause of this lax privacy attitude can be identified as the social media platforms themselves because they encourage sharing excessive amounts of personal information (Tsay-Vogel, et al., 2018). Moreover, users might have a relaxed attitude towards privacy because of their social media activity patterns, the increased satisfaction they receive from disclosure and psychological mechanisms (Debatin, et al., 2009).

Taken together these studies lead to the conclusion that attitude significantly influences information disclosure intention. Furthermore, in relation to the Privacy Calculus theory, a user's attitude towards disclosure influences the strength of their perceptions regarding the risks and benefits involved when disclosing information online. In other words, users might have a predisposition to overestimate either the risks or the benefits of self-disclosure. If a user has a negative attitude towards disclosure, they might be more inclined to perceive increased risks while users who have a positive attitude towards disclosing information might perceive increased benefits.

4.2.3 The Privacy Paradox

When examining privacy attitude an interesting phenomenon to note is the privacy paradox which refers to the inconstancies that exist between a person's attitude and behaviour (Barth & De Jong, 2017). Users can share, like, comment and post anytime day or night, as social media and the Internet provide 24/7 access to information, entertainment and other content. Consequently, online engagement has become a daily habit and this constant connection online poses various threats to a user's privacy and security (Barth & De Jong, 2017). As seen in section 3.2.4 users are generally motivated to disclose information by the potential rewards, they might gain such as social capital, convenient relationship management, self-presentation and entertainment, regardless of the risks to the privacy of their personal information. Nevertheless, evidence has been found that individuals are concerned about their online privacy (Debatin, et al., 2009; Smith, Dinev & Xu, 2011; Mahmoodi, et al., 2018). Thus, users often claim they care about the privacy of their information, but they will reveal personal data for minor rewards (Kokolakis, 2017).

Interestingly, there is a debate as to whether the privacy paradox actually exists. Several studies have found evidence that the privacy paradox does in fact exist (Norberg, Horne & Horne, 2007; Taddicken, 2014; Lee, Park & Kim, 2013; Taddei & Contena, 2013), while others found no support for this phenomenon (Debatin, et al., 2009; Dienlin & Trepte, 2015; Joinson, et al., 2010). For instance, Norberg, et al. (2007) found users disclosed far more information than their expressed intentions. This suggests that intention might not lead to actual behaviour when it comes to privacy (Norberg, et al., 2007). Similarly, the attitude-behaviour gap has also been confirmed by Lee, et al. (2013) who determined that users share personal information even though they have a highly concerned attitude regarding their privacy. This is because users take into consideration both risks and benefits and adapt their

information control strategies to maximize benefits and minimize risks (Lee, et al., 2013). Furthermore, Taddei and Contena (2013) determined that privacy concerns have a direct effect on self-disclosure. On the other hand, some studies found that privacy behaviour might not be paradoxical after all. Joinson, et al., (2010) concluded that privacy concerns predicted whether a user would disclose personal information online. Likewise, Stutzman, et al., (2012) found support for the relationship between privacy attitude and disclosure, as well as privacy attitude and privacy behaviour. Moreover, Dienlin and Trepte (2015) found that when differentiating between privacy attitude and privacy concerns, as well as applying the Theory of Planned Behaviour the privacy paradox can disappear.

This debate has prompted researchers to investigate the cause of the paradox and the solutions that could resolve this phenomenon. Research done in this area has interpreted the paradox by either constructing models or by attempting to explain this phenomenon (Kokolakis, 2017). One proposed explanation of this paradoxical privacy behaviour is that user's make privacy decisions based on incomplete information which makes them overestimate the benefits and underestimate the risk their personal information (Kokolakis, 2017). It has also been argued that users lack awareness of both privacy threats and how to protect their information online (Acquisti, et al., 2015; Barth & De Jong, 2017). Furthermore, Hoffmann et al. (2016) proposed that the discrepancy between attitude and behaviour could be explained by privacy cynicism. This is because privacy cynicism permits users to engage in online platforms although they are aware of the risk to their privacy and have no trust in the platform's provider because they believe they have no control over protecting their data (Hoffmann, et al., 2016).

Furthermore, due to the context-dependence of privacy decisions, users can display an attitude towards privacy that ranges from severely concerned to indifferent depending on the specific situation (Acquisti, et al., 2015). A further explanation for the privacy paradox might be related to subjective norms. Users might feel pressured to disclose personal information in order to reciprocate the sharing of others (Kokolakis, 2017). Thus, a user's actual behaviour reflects public opinion and the user's attitude refers to their unbiased opinion (Trepte & Dienlin, 2014; Kokolakis, 2017). In other words, a user might continue to disclose information even although they have a concerned attitude because disclosing information is the norm.

Currently, there are no practical solutions to bridge the gap between attitude and behaviour (Barth & De Jong, 2017). Instilling a sense of psychological ownership amongst users could result in them feeling a sense of responsibility to keep their personal information safe. To develop this psychological ownership users must increase their risk perception and think of themselves as vulnerable to privacy threats and not simply attribute these threats to others (Barth & De Jong, 2017). Some other solutions include providing users with enough information to make informed decisions through the use of privacy awareness tools (Pötzsch, 2009) and creating interfaces that elicit privacy-protective behaviours (Kehr, et al., 2015a).

Additionally, while there is evidence that negates the existence of the privacy paradox, the researcher in this study is of the notion that the privacy paradox does exist and is thus in agreement with Norberg, et al. (2007), Lee, et al. (2013) and Taddicken (2014).

4.2.4 Factors Influencing Attitude Towards Disclosing Information Online

While there is a debate about whether privacy attitude can play a role in a user's privacy-protective behaviour it is still useful to understand the factors that influence and predict a user's attitude towards information sharing. These factors are identified and discussed below.

4.2.4.1 Experience

Privacy attitude is often a result of past experience and a change in the user's environment can activate privacy concerns (Acquisti, et al., 2015). Thus, when a user suffers a privacy invasion, they tend to have a negative attitude towards sharing information and are more concerned about their privacy. Users are more inclined to have a concerned attitude when they have personally experienced an online privacy violation than when their attitude towards privacy is based on second-hand experiences (Gerber, et al., 2018). This is because attitudes based on personal experience lead to more consistent attitudes than those based on the experiences of others (Tormala, Petty & Briñol, 2002). Debatin, et al. (2009) found that 80% of users who experienced a privacy infringement changed their settings on Facebook in comparison to only 42% who changed their settings after hearing about the privacy violations of others. However, after a while user's adapt and become habituated to the existence and surveillance of technology (Acquisti, et al., 2015). For instance, users might realise their phone is listening to them and recording their data but ascribe this to the price one pays for the convenience of technology. In relation to attitude towards privacy-

protective behaviour, Yao (2011) noted that the more concerned a user is about potential privacy infringements, the more likely they will be to have a positive attitude towards privacy-protective strategies. Thus, past experiences influence a user's attitude towards disclosure online.

4.2.4.2 Perception of risk and benefit

Another factor influencing a user's attitude towards information disclosure online is their perception of the risks and benefits involved. Attitude towards self-disclosure online is established by the perceived risks and benefits of the disclosure behaviour and the strength of these perceptions in a specific context decide the individual's general attitude in that context (Li, 2012). Users will have a more positive attitude towards disclosing personal information online when they are offered benefits (Robinson, 2018). This might be because users will disclose information when they have a reason to disclose (Heirman, et al., 2013). In the context of social networking, these reasons include enjoyment and to maintain relationships. Benefits often motivate users to behave in a way that is in conflict with their privacy attitudes (Robinson, 2018). For instance, Debatin, et al. (2009) concluded that even when a user experienced a privacy infringement, the benefits of engaging on Facebook offset the privacy concerns. This finding might be explained by the level of infringement that has occurred. Thus, a low-level infringement such as profiling might not cause as much concern as a high-level infringement such as online identity theft.

On the other hand, perceived risk has been found to influence a user's attitude towards information disclosure online in a negative way. A higher perception of privacy risks will reduce positive attitudes toward information disclosure online (Hajli & Lin, 2016). Thus, assessments of risk play a role in a user's attitude towards disclosure and their willingness to disclose information (Tsay-Vogel, et al., 2018). Moreover, a high perception of risk predicts higher levels of privacy concern (Gerber, et al., 2018). In other words, users who perceive higher risks to the privacy and security of their data are likely to have a more concerned attitude towards their personal data. In a study investigating the factors that influence information disclosure attitude on e-commerce platforms, Robinson (2018) concluded that increased perceptions of risk lead to anxiety and in turn fosters a negative attitude towards disclosing information online. In summation, perceived benefits lead to a positive, open attitude towards disclosing information online, while perceived risks lead to a negative, sceptical attitude towards disclosing information online.

4.2.4.3 Trust

The next factor that influences attitude towards information disclosure is trust. Trust can be defined in this study as "the firm belief in the competence of an entity to act dependably, securely and reliably within a specified context" (Grandison & Sloman, 2000). Thus, trust refers to accepting a situation that could place one in a vulnerable position based on the expectation that others will behave in an ethical manner (Chang, et al., 2017). This concept can be further conceptualized as the willingness to disclose information based on the expectation that platforms such as Google, Facebook and Instagram will keep this personal information private and safe. The creation of trust online is a complex process and once created, it can alleviate uncertainty, vulnerability and risk perceptions that are related to personal information disclosure (Mesch, 2012). Additionally, trust propensity was found to predict adolescent attitudes toward disclosing information online (Heirman, et al., 2013). As such, users who are inclined to be more trusting have a positive attitude towards disclosing information online (Heirman, et al., 2013). Furthermore, trust, in general, is a good predictor of a user's attitude towards information disclosure online (Robinson, 2018).

Trust can also be discussed in relation to Uncertainty Reduction Theory, as trust soothes a user's perception of risk and uncertainty leading them to engage in trusting behaviours (McKnight, Choudhury & Kacmar, 2002). Uncertainty reduction theory states that exchanging information with others allows an individual to reduce their uncertainty about another person and thereby form an impression of that person (Palmieri, et al., 2012). This results in individuals being able to predict the behaviour of others which can lessen the anxiety of initial interactions (Palmieri, et al., 2012). This idea can be translated from face-to-face communication to online interaction, as users can reduce their uncertainty about others by disclosing information about themselves in the hopes that others will do the same. The more disclosure that occurs between users, the more they can predict the behaviour of the other person, which leads to an increased level of trust in that member and, in turn, leads to further disclosure (Sheldon, 2009). Thus, the more users disclose, the more trust is built and the less uncertain users feel towards their online network (Sheldon, 2009). Furthermore, social media platforms are also useful in facilitating information-seeking behaviour which acts as a strategy to reduce uncertainty and tends to increase information disclosure (Lin, et al., 2016).

In the context of self-disclosure on social networking sites, trust can be broken down into two components, namely, trust in social network members and trust in the social network platform. Krasnova, et al., (2010) found that trust in social network members did not lessen perceived risk. Interestingly, Lo and Riemenschneider (2010) determined that while trust in a user's friend group influences willingness to disclose, no relationship exists between trust in all social network members and a user's willingness to disclose personal information online. Intersetingly, Krasnova, et al. (2012) concluded that both trust in social network members and trust in the social network platform influences a user's intention to disclose. As users gain trust in their friend network to guard shared personal information, they have a more open attitude towards disclosing more information (Millham & Atkin, 2018). The trust users have for their friend network might be explained by the idea that disclosing information with other people makes them responsible for the protection of this information, as they are "co-owners" joint owners (Acquisti, et al., 2015). Additionally, one of the best predictors of privacy attitude is trust in the website or platform (Gerber, et al., 2018). Users are more likely to have a positive attitude towards sharing and disclose more personal data when they trust Facebook (Chang & Heo, 2014). Trust in the website significantly predicts a user's level of information disclosure (Bevan-Dye & Akpojivi, 2016). Thus, trust in the platform reduces concerns and fosters a positive attitude towards information disclosure online.

4.2.4.4 Computer Anxiety

Following trust in the platform, computer anxiety has also been found to be one of the best predictors of a user's attitude towards information disclosure (Gerber, et al., 2018). Computer anxiety refers to a fear of engaging with a computer or technology both immediately or in the future (Blignaut, et al., 2009). A user's attitude towards the handling of their information by companies and online platforms is influenced by computer anxiety. Gerber, et al., (2018) determined that computer anxiety predicts a user's attitude towards the information practices of a corporation. Additionally, users with higher computer anxiety have a more concerned attitude towards their information (Schwaig, et al., 2013). This increased concern for their information leads to a lower intention to disclose personal information. Furthermore, due to their fear of interacting with computers, these users anticipate increased threats to their information, which cultivates a negative privacy attitude. Thus, computer anxiety negatively influences a user's attitude toward self-disclosure.

4.2.4.5 Perceived Control

Finally, perceived control also influence's a user's attitude towards information disclosure. The addition of privacy settings to social media platforms and websites have been found to alleviate concerns about privacy and disclosure (Stutzman, et al., 2011). Hajli and Lin (2016) determined that perceived control leads to an increased positive attitude towards information disclosure in females rather than males. Furthermore, control can lead to users disclosing far more information than they intended because perceived control decreases a user's concerned attitude (Acquisti, et al., 2015). Thus, an increased perception of control over information leads to a positive attitude towards disclosure because the user is not so anxious about the data collected from the posts they share on social media (Hajli & Lin, 2016).

Figure 4.2 provides an illustration of the factors that influence a user's attitude towards disclosing information online.

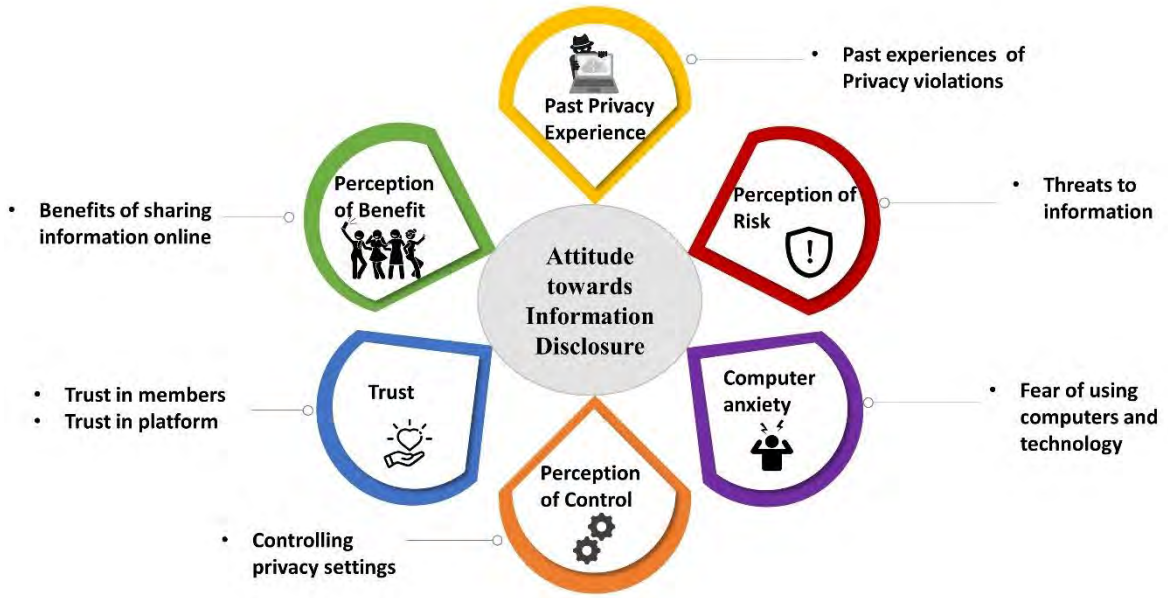


Figure 4.2 Factors Influencing Attitude Towards Information Disclosure

4.2.5 Subjective Norms and Information Disclosure

Subjective norms are important to discuss when investigating information sharing behaviours (Lutz, et al., 2018). Often used interchangeably, subjective norms or social influence refer to a user's perception of the expectations of others related to a specific behaviour such as information disclosure (Lutz, et al., 2018). Users often look to their environment and the people around them for guidance when they are uncertain about their privacy preferences (Acquisti, et al., 2015). Thus, when users see other individuals disclosing personal information, they will be more inclined to disclose personal information about themselves (Acquisti, et al., 2015). Various norms can be observed regarding online emotion expression, with many posts on social media leaning towards being positive instead of negative (Reinecke & Trepte, 2014). For example, "overly emotional" posts online seem to go against the unspoken norms of self-disclosure and leave others describing this excessive disclosure as "gross" and "weird" (Lambert, 2016, p. 10). Interestingly, expressing negative emotions such as anger, worry, disappointment or sadness is more suited to Facebook rather than Instagram (Waterloo, et al., 2018). Yet, the expression of pride and joy are seen as appropriate for both Facebook and Instagram (Waterloo, et al., 2018). In the context of social networking, individuals have to tread the fine line between disclosing enough information to maintain their relationships, while still not revealing too much personal information. As such, norms are useful in regulating self-disclosure behaviour (Zillich & Müller, 2019). For instance, to manage the issue of protecting privacy while self-disclosing, most users censor their posts about their daily lives and are very selective when choosing their Facebook friends (Zillich & Müller, 2019). These privacy-protective strategies are not only established on an individual level but are also consolidated through collaboration with others and are thus based on norms (Zillich & Müller, 2019). Table 4.1 provides some useful definitions to facilitate a better understanding of the different types of norms influencing behavioural intention.

Table 4.1 Definition of Norms

Term	Definition
Subjective Norms	"The perceived social pressure to perform or not perform the behaviour" (Ajzen, 1991, p. 188). These norms refer to performing behaviours based on what is expected by society (Cialdini & Trost, 1988).
Injunctive Norms	These norms refer to what others disapprove or approve of (Cialdini, et al., 2006).
Descriptive Norms	These norms refer to "what is commonly done" (Cialdini, et al., 2006, p. 4)
Social Norms	"Social norms are rules and standards that are understood by members of a group and that guide and/or constrain social behaviour without the force of laws" (Cialdini & Trost, 1988, p. 152).

Thus, descriptive norms are a user's perception of what other people normally do, injunctive norms are a user's perception of whether other people will approve or disapprove of their behaviour and subjective norms refer to how important people in the user's life expect them to behave. Together, these three norm types, along with a user's own expectations of behaviour form overarching social norms (Cialdini & Trost, 1988).

Subjective norms have been seen to influence a user's intention to disclose information online and actual disclosure behaviour. The social pressures applied by important peers is the most significant factor that predicts an adolescent user's intention to disclose information of a personal nature (Heirman, et al., 2013). Interestingly, in relation to sharing information about other people online, social norms were not a significant predictor of intention to disclose (Koohikamali, Peak & Prybutok, 2017). Additionally, peer pressure is also a strong determining factor when it comes to the use of social networking platforms and other online activities (Koroleva, et al., 2011). A reason for this is that the use of social media platforms announce a user's membership to a social group and through this affiliation a user learns the appropriate and expected behaviours of that group (Varnali & Toker, 2015). This is done by gaining cues from the profiles of online friends and their disclosure practices (Varnali & Toker, 2015). Consequently, subjective norms have been identified as influencing the regularity of sharing and decreasing concerns about the privacy of information (Lutz, et al., 2018). This is because the norm of reciprocity fosters increased information sharing and can outweigh concerns about the privacy of a user's personal data (Lutz, et al., 2018). On the other hand, privacy social norms have been found to reduce information disclosure when significant peers assist in raising a users awareness regarding potential threats to their data, the less that user will self-disclose (Zlatolas, et al., 2015).

In a study predicting privacy protection online, both descriptive and injunctive subjective norms were found to influence intentions (Saeri, et al., 2014). When users observe their peers putting privacy protection strategies in place or approving of protecting privacy online, they have an increased intention to protect their own privacy (Saeri, et al., 2014). Moreover, subjective norms have also been found to positively influence the disclosure of personal information such as contact details, as well as the disclosure of, among other things, opinions, thoughts and memories (Varnali & Toker, 2015). This is because a user's perception of privacy and their intention to disclose is influenced by others (Kaushik, Jain, & Singh, 2018). The important role subjective norms play in relation to intention is further illustrated by Chang and Chen (2014), who determined that students were more likely to disclose their location information on Facebook if the friends in their network were disclosing their locations. Additionally, subjective norms have a greater effect on self-disclosure behaviour in comparison to perceived risks and benefits (Cheung, et al., 2015; Wirth, et al., 2019). Users are inclined to self-disclose more in order to conform to the expectations of their friend network (Cheung, et al., 2015). Thus, the influence of others can override privacy concerns.

Overall, these findings highlight the significant role subjective norms play in determining both a user's intention to disclose personal information online and their actual disclosure behaviour.

4.2.6 The Fear of Missing Out Phenomenon

The pervasiveness of social media has made it easy for users to stay connected and informed about the lives of others, which can result in a fear of missing out (FOMO) (Dogan, 2019). This phenomenon refers to a severe "apprehension that others might be having rewarding experiences from which one is absent" (Przybylski, et al., 2013, p. 1841). Thus, users have a strong need to avoid social isolation by engaging on social media platforms despite their privacy concerns (Jeong & Kim, 2017). This phenomenon mostly affects young adults, who feel pressured by their friends, family and significant others to maintain relationships round-the-clock on social media platforms (Fox & Moreland, 2015). As subjective norms are determined by perceived social pressures that influence behaviour(Beyens, Frison & Eggermont, 2016), FOMO could influence a user's perception of the subjective norms related to disclosure. Thus, increased levels of FOMO will increase a user's susceptibility to comply with the subjective norms of their peer group.

The effects of FOMO also have an impact on a user's privacy attitude. In a study on the online risk-taking of adolescents, Popovac and Hadlington (2019) determined that FOMO is one of the main predictors of risk-taking online such as accepting unknown friend requests. Furthermore, FOMO has been found to urge users to disclose more information and increase their usage of social media platforms (Beyens, et al., 2016; Buglass, et al., 2017). In particular, users who have high levels of FOMO are more inclined to compulsively check social media sites such as Instagram, Facebook, MySpace and Twitter (Abel, Buff & Burr, 2016). This is because these users are trying to avoid suffering from the negative feelings of being left out (Jeong & Kim, 2017). This fear of missing out further leads to users disregarding their privacy concerns, even when they are aware of privacy threats, due to a need to remain involved and informed about their friend's activities (Fox & Moreland, 2015). As such, a higher level of FOMO will foster a careless attitude towards the privacy of personal information because users are focussed on avoiding social isolation.

In summation, FOMO can be seen to influence both subjective norms and privacy attitude. While this phenomenon has been investigated in relation to psychological wellbeing and problematic social media use (Buglass, et al., 2017; Franchina, et al., 2018), not a lot of attention has been paid to how this phenomenon's influence on a user's subjective disclosure norms and intention to disclose personal information online. Thus, further investigation into the relationship between FOMO and intention to disclose personal information, mediated through subjective norms could shed new light on online self-disclosure.

4.2.7 Perceived Behavioural control

The final construct with the Theory of Planned Behaviour that influences behavioural intention is perceived behavioural control. Perceived behavioural control refers to the ease or difficulty of performing a behaviour. In the context of personal information disclosure, this would determine whether the user views disclosure or non-disclosure as an easy or difficult task. Essentially, behavioural control is the person's ability to perform the behaviour while intention is the motivation to perform the behaviour (Ajzen, 1991). Moreover, the execution of the behaviour is reliant on the availability of resources such as time, skills and finances, which form the actual control over the behaviour a person possesses (Ajzen, 1991). Thus, while the user might be motivated to protect their privacy online and believe it to be an easy task, they could lack the skills and time needed to adjust their privacy settings.

Perceived behavioural control is derived from self-efficacy which is found in Social Cognitive Theory. Self-efficacy refers to an individual's judgements of their "capabilities to organize and execute the courses of action required to produce given levels of attainments" (Bandura, 1998). These concepts are similar in the sense that they both revolve around an individual ability to execute behaviours (Ajzen, 2002). To avoid confusion surrounding whether perceived behavioural control refers to control over an outcome or control over the execution of a behaviour, this construct can be thought of as "perceived control over performance of a behaviour" (Ajzen, 2002, p. 668).

Within the Theory of Planned Behaviour perceived behavioural control is seen to influence both intention and actual behaviour (Ajzen, 1991), however, in some studies within an online context this was not the case. For instance, Heirman, et al. (2013) found that perceived behavioural control was not a significant predictor of intention disclosure among adolescents, possibly because these users have computer and Internet usage skills that foster an increased sense of control. This study did, however, find that perceived behavioural control did have a positive influence on actual behaviour (Heirman, et al., 2013). Similarly, perceived behavioural control was a good predictor of "online safety behaviour" but not behavioural intention (Burns & Roberts, 2013, p. 59). Furthermore, Taneja, et al. (2014) concluded that perceived behavioural control did not have a significant influence on a user's intention to use privacy controls. This might be because users understand that if they would like to use privacy controls, they have the ability to do so (Taneja, et al., 2014). Likewise, in a study investigating privacy protection online perceived behavioural control was not a predictor of a user's intention to protect their privacy online (Saeri, et al., 2014). While some studies did find that perceived behavioural control influences behavioural intention (Jafarkarimi, et al., 2016; Kim, et al., 2016), it will be useful to adapt the Theory of Planned Behaviour to the online context through the addition of privacy awareness. The replacement of perceived behavioural control with privacy awareness seems appropriate as privacy awareness allows users to make informed decisions regarding self-disclosure online (Pötzsch, 2009). Moreover, it is imperative to determine a user's privacy and information security awareness level, as there is a significant relationship between awareness and actual behaviour (Öğütçü, Testik & Chouseinoglou, 2016). This further supports the replacement of perceived behavioural control with awareness because both these constructs have an influence on intention and a direct influence on actual behaviour. Besides this similarity between the two constructs, Van der Schyff and Flowerday (2019) found sufficient evidence

for a model based on the Theory of Planned behaviour that replaced perceived behavioural control with information security awareness in a social media context.

Additionally, privacy awareness can function as both a control belief and a behavioural control. As a control belief, privacy awareness could increase a user's perception of the factors that either facilitate or impede the execution of the behaviour (Ajzen, 2002), and in turn, this perception would influence whether a user regarded the behaviour as being easy or difficult to perform. In other words, if the user is aware of the risks related to disclosure, they would perceive disclosure as being more difficult, whereas if the user lacks awareness of threats but has increased awareness of the benefits of disclosure, they would perceive disclosure as being easy and advantageous. Essentially, a user can control their disclosure based on the level of awareness they possess.

4.2.8 Awareness and Information Disclosure

Despite frequent warnings and reports of data and security breaches, many users do not engage in secure online behaviour (Shillair, et al., 2015). A reason for this is that users lack knowledge surrounding strategies to prevent vulnerabilities and alleviate threats online (Guedes, et al., 2016b). For example, in a study on Facebook privacy awareness, 88% of respondents stated they have never used or modified their privacy settings which place their data in a vulnerable position (Nyoni & Velempini, 2018). Furthermore, users are often unaware that the information disclosed on social media is gathered and stored by the platform (Zlatolas, et al., 2015). For instance, users might be unaware of the personal data that is automatically collected about them by Google and Facebook through online searches and cookies (Esteve, 2017). Interestingly, a study on online behavioural tracking found that while most users are aware that companies such as Google and Facebook can gather data about their online activities, this awareness leads to lower levels of concern (Rader, 2014). However, an awareness of potential inferences that can be made based on this behavioural tracking such as association with a political party was related to an increased level of concern (Rader, 2014). Thus, if users are more aware of the inferences that can be made based on their online behaviour they might behave in a more cautious way.

Van der Schyff & Flowerday (2019) argued that users who have sufficient knowledge and therefore increased awareness of privacy threats protect their information online due to a positive attitude towards securing their data. For instance, an increased awareness of threats to online information positively influences password strength (Mamonov & Benbunan-Fich,

2018). Moreover, increased privacy awareness has a significant negative impact on both privacy concerns and information disclosure online (Zlatolas, et al., 2015). Thus, the more aware users are about privacy threats and the potential secondary disclosure of their personal data, the more concerned they will be and thus they will have a lower intention to disclose information (Zlatolas, et al., 2015). Similarly, Padyab, et al. (2019) concluded that after users were made aware of the inferences that can be made about them based on their social media profiles, they felt the need to be more careful and cautious when disclosing information online. Furthermore, higher levels of privacy concern motivate users to increase their knowledge surrounding the risks related to excessive self-disclosure online (Fatima, et al., 2019). In turn, this increased privacy awareness leads to more restricted disclosure in the long run (Fatima, et al., 2019). Consequently, might be possible to modify a user's privacy behaviours by increasing both awareness on the risks of information disclosure and awareness of specific data breaches and infringement cases on social media sites (Newk-Fon Hey Tow, Dell & Venable, 2010). On the other hand, Ampong, et al. (2018) found that even when users had an increased awareness of privacy problems and threats, they continued to disclose vast amounts of information online. This continued disclosure despite privacy awareness might be because these users ensure their online friend network consists of people they know (Stutzman, Gross & Acquisti, 2013) and they make use of privacy settings.

Overall, these studies highlight the important role privacy awareness plays when it comes to information disclosure. Privacy awareness significantly influences both a user's intention to disclose and their actual disclosure online. Furthermore, in relation to the Privacy Calculus theory, a users level of awareness will increase the strength of their perceptions regarding the risks and benefits involved when disclosing information online. The more aware a user is of the threats to their data and the inferences made by platforms based on this data, the more cautious they will be and the less information they will willingly disclose. On the other hand, a lack of awareness regarding the threats to personal data will increase disclosure and could strengthen a user's perception of the benefits related to disclosure as they are unaware of the threats this disclosure poses.

4.2.9 Personal Valuation of Information

One aspect that influences both privacy awareness and attitude is a user's personal valuation of their data. When a user becomes aware that their personal data can be a tradeable asset the valuation of their personal data changes (Spiekermann & Korunovska, 2017). Once users learn that their personal data can be harvested and traded with third-parties, they perceive this data as having more value and are more reluctant to share this data (Spiekermann, et al., 2012). Interestingly, while higher levels of privacy concern do not automatically cause a user to have an increased valuation of their personal data, increased awareness of personal data as tradable asset leads to users being more concerned about privacy (Spiekermann, et al., 2012). This, in turn, influences users to actively protect their data.

Another factor that significantly influences a user's valuation of their information is psychological ownership. Once people build a sense of psychological ownership towards their data, they attribute it with increased value (Spiekermann & Korunovska, 2017). This is because people are inclined to attach a higher value to the things they own rather than things they do not own (Van Lieshout, 2014). Thus, the more users engage and share information online, the more value they assign to the data they share and the more inclined they are to protect this data (Spiekermann & Korunovska, 2017). Besides increasing a user's perception of value related to their personal data, psychological ownership also drives users to protect their data from deletion (Spiekermann, et al., 2012). Moreover, if a person has a higher valuation of their information, specifically a high sense of ownership towards their data, they will be more concerned about their privacy (Millham & Atkin, 2018). Additionally, Bauer, et al. (2012) determined the size of a user's friend network also influences the valuation of personal information. Consequently, the larger the friend network the more the user values their information (Bauer, et al., 2012). Overall, this valuation of personal information informs a user's attitude towards disclosure (Millham & Atkin, 2018). If they feel a strong responsibility to keep their information private because they own it, they will disclose less.

Taken as a whole, these findings suggest that a user's personal valuation of their information will influence their attitude towards disclosure and their level of privacy awareness. If a user values their data more, they will stay informed regarding privacy threats and they will have a more cautious attitude towards disclosure. Additionally, the more aware the user is that their personal data has value, the more they will actively protect this data.

4.3 Summary

This chapter thoroughly discussed the core aspects of the Theory of Planned Behaviour in relation to a user's intention to disclose information online. This discussion was taken a step further by incorporating the antecedent factors of *Trust in the Social Media Provider*, *FOMO* and *Personal Valuation of Information*. Overall, it was determined that attitude, subjective norms and privacy awareness significantly influence a user's intention to disclose information online. Moreover, each of these constructs has an effect on the strength of a user's perception regarding the risks and benefits involved when disclosing information online. As such, a research model was created illustrating the mediating effect of the Privacy Calculus Theory when combined with the Theory of Planned Behaviour. The next chapter will cover the theoretical propositions of this study.

CHAPTER 5: THEORECTICAL PROPOSITIONS AND PROPOSED MODEL

5.1 Introduction

This chapter starts by providing a discussion of the motivation behind the creation of the three propositions in this study. Based on the literature reviewed and the research questions a proposition was created for attitude, subjective norms and awareness. The findings from chapter 3 and 4 also lead to the creation of a proposed model which is explained towards the end of this chapter.

5.2 Theoretical Propositions

5.2.1 Attitude

Attitude refers to the extent to which an individual considers performing a specific behaviour as either being positive or negative (Ajzen, 1991). Section 4.2.2 in the previous chapter determined that privacy attitude significantly influences information disclosure intention. If a user has a positive attitude towards sharing information, they will be more likely to self-disclose online, whereas if a user has a negative attitude towards sharing information, they will be less likely to self-disclose online. According to Chang, Wong and Lee (2015) users often balance a positive, trusting attitude against a negative concerned attitude when it comes to assessing the perceived privacy of their online information. When users perceive more benefits, they have a more positive attitude towards disclosure and thus will be more inclined to disclose personal information online (Robinson, 2018). As such, individuals perceiving more benefits regarding sharing information have a less concerned attitude towards privacy (Steijn, et al., 2016). On the other hand, when users are more anxious regarding disclosure due to the perceived risk to their data, they have a negative attitude towards disclosure and are less likely to disclose personal information online (Robinson, 2018). Consequently, attitude towards disclosing information is determined by the perception of the risks and benefits of disclosure, while the user's overall attitude determines whether benefits will outweigh the risks in a given context (Li, 2012).

Taken a step further, users might have a predisposition to overestimate either the risks or the benefits of self-disclosure. For example, a study on the influence of mood on the privacy calculus found that users with a positive mood overestimated the benefits of disclosure and

underestimated the risks of disclosure (Alashoor & Al-Jabri, 2018). These users had a more positive attitude towards disclosure due to their positive mood and thus perceived more benefits to disclosure. Mood states have been shown to influence attitude through behavioural beliefs and can have effects on both evaluation and the strength of beliefs (Ajzen, 2011). Additionally, a concerned attitude towards privacy will enhance risk perceptions, while a trusting attitude will reduce risk perception and increase benefit perception (Kehr, Wentzel, & Kowatsch, 2014). Thus, a user's attitude has an influence on their risk and benefit perceptions. If a user has a negative attitude towards disclosure, they might be more inclined to perceive increased risks while users who have a positive attitude towards disclosing information might perceive increased benefits. As such, it is proposed that:

> **Proposition 1**: *Attitude towards disclosure will influence a user's perception regarding the risks and benefits involved when disclosing online.*

This proposition corresponds to the relationships between attitude and perceived risk, as well as attitude and perceived benefits. This is depicted the proposed model in Figure 5.1 as P1.

5.2.2 Subjective Norms

Subjective norms are defined as a person's perception of social pressures that encourage or discourage behaviour (Ajzen, 1991). Since subjective norms can influence a user's intention to disclose information in a positive or negative way, these norms also influence a user's perception of the benefits and risks related to information disclosure. Peer pressure affects a user's perception of both risks and benefits related to using social media and disclosing information on social media (Koroleva et al., 2011). If the most influential people in a user's peer group believe that frequent information disclosure provides many benefits, it would make the user disclose personal information in order to gain these benefits. Lutz, et al. (2018) determined that subjective norms significantly increase a user's perception of the benefits related to sharing information online. This is because a user's perception of the benefits related to information sharing is essentially dependent on the approval and reassurance of their peers (Lutz, et al., 2018). Furthermore, the subjective norms related to using social media platforms can act as an enticement to comply with the social influence of others (Min & Kim, 2015). Users subscribe to and engage on social media platforms that their friends and peers use. Similarly, if friends and peers disclose their personal information

users feel pressured to do the same because of a fear of suffering social disapproval or being labelled as having something to hide (Kokolakis, 2017).

On the other hand, subjective norms can also influence a user's risk perception, as mentioned in Chapter 3. The more users perceive the norm to be privacy-conscious, the more they will endeavour to protect their information and self-disclose less. For instance, users are more inclined to use privacy controls if their friend network expects them to use these controls (Taneja, et al., 2014). Furthermore, if a user's friends and peers are concerned about their privacy, the user is likely to increase their privacy literacy and disclose less information (Nouh, et al., 2014). In turn, an increase in their privacy literacy will increase their risk perception. Moreover, adolescents have been found to emulate the Facebook privacy settings of their peers (Hofstra, Corten, & van Tubergen, 2016). For example, users are more inclined to set their Facebook profiles to private if their peers have private profiles (Hofstra, et al., 2016).

These findings suggest that subjective norms influence a user's risk and benefit perception. If the most influential people in a user's peer group believe that information disclosure provides many benefits, it will influence the user to disclose personal information to gain these benefits. Alternatively, if the most influential people in a user's peer group believe that information disclosure poses various risks to their personal information, it would influence a user to disclose less personal information. Thus, it is proposed that:

> **Proposition 2**: *Subjective norms influence a user's risk and benefit perception when disclosing information online.*

This proposition corresponds to the relationships between subjective norms and perceived risk, as well as subjective norms and perceived benefits. This is depicted in the proposed model in Figure 5.1 as P2.

5.2.3 Awareness

In this study the Perceived Behavioural Control construct from the original Theory of Planned Behaviour is replaced with privacy awareness. This replacement seems appropriate because privacy awareness allows users to make informed decisions regarding self-disclosure online (Pötzsch, 2009). Furthermore, in an online context, awareness of privacy related issues and threats is essential to the protection of personal information. This is because awareness can assist users when making decisions regarding what countermeasures

to take against potential threats (Malandrino, et al., 2013). As a behavioural control, awareness would determine whether a user regarded disclosing information as being either easy or difficult. If the user is aware of the risks related to disclosure, they would perceive disclosure as being more difficult, whereas if the user lacks awareness of threats but has increased awareness of the benefits of disclosure, they would perceive disclosure as being easy and advantageous. Thus, they can control their disclosure based on the level of awareness they possess.

The rise of computers and the Internet has led to new opportunities for cybercrime (Bregant & Bregant, 2014). However, while cyber-threats have increased and evolved, many users still have a limited awareness and understanding regarding the vast variety of threats on the Internet (Furnell & Moore, 2014). This lack of awareness extends to interactions on social media as users are unaware of the way in which their information is harvested and used by third parties and online platforms (Benson, et al., 2015). On the other hand, users who have sufficient knowledge and therefore increased awareness of privacy threats are more likely to protecting their information online. Furthermore, users who are aware of privacy threats disclose less information on social media (Acquisti & Gross, 2006). A more in-depth discussion of the influence of awareness on information disclosure can be found in chapter 4, section 4.2.8. Additionally, it has been shown that once users are made aware of the value they attach to their information, they are more inclined to protect their data. As seen in section 4.2.9, once users learn that their personal data can be harvested and traded with third-parties, they perceive this data as having more value and are more reluctant to share this data (Spiekermann, et al., 2012). Following this increase in awareness, the user will be more inclined to protect their information and limit their disclosure. Additionally, users who have increased awareness of privacy threats will perceive more risks and thus disclose less information online. Therefore, it is proposed that:

> **Proposition 3:** *Increased privacy awareness will reduce information disclosure online.*

This proposition corresponds to the relationships between awareness and perceived risk, as well as perceived risk and intention to disclose personal information online. This is depicted in the proposed model in Figure 5.1 as P3.

5.2.4 Proposed Model

Based on the findings in chapter two, three and four the following model in Figure 5.1 was created. This model has both primary and secondary constructs. The primary constructs, in black, serve as the main model of the study while constructs in blue are antecedent constructs that provide further insight into the primary model. The model depicts a combination of the Theory of Planned Behaviour and the Privacy Calculus Theory. In this model, the constructs in the Privacy Calculus Theory serve as factors mediating the constructs within the Theory of Planned Behaviour.

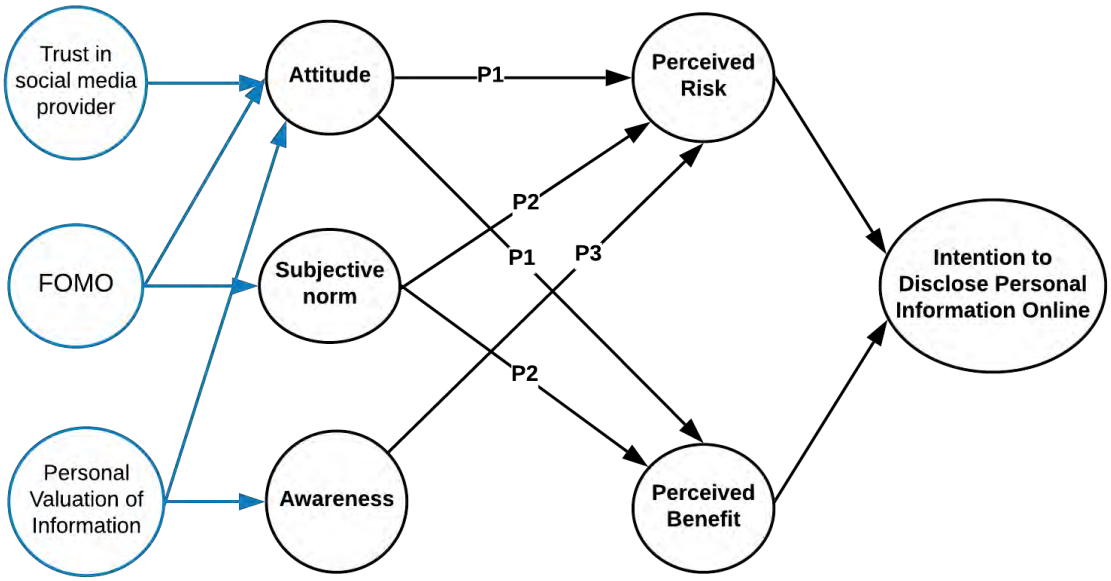


Figure 5.1 Proposed Model

The model proposes that the *Intention to Disclose Personal Information Online* results from analysing the *Perceived Risks* and *Perceived Benefits*. Thus, if the benefits are perceived as being more than the risks users will disclose and if users perceived increased risks, they will limit disclosure. The model shows that when perceiving the risks and benefits of disclosure users are influenced by their *Attitude, Subjective norms* and their level of *Awareness*. Finally, the constructs in blue show the antecedents that have an impact on a user's attitude, their subjective norms and their level of awareness.

5.3 Summary

Social media can provide users with many benefits, but using these platforms can lead to negative consequences both online and offline (Alqatawna, et al., 2017). While many users engage online daily, they remain unaware of how their personal information is retrieved and used (Kang, et al., 2015). As such, this study aims to determine what drives continued disclosure online and whether an increase in awareness of the value of personal information motivates users to safeguard their information. To this end, a discussion of the motivation behind the creation of the three propositions and the proposed model has been provided. Rationale was given for the creation of each proposition which is depicted in the proposed model in Figure 5.1. This model is derived from the theoretical foundation of this study and thus illustrates the combination of the Theory of Planned Behaviour and the Privacy Calculus Theory. The next chapter will cover the research methodology of this study.

CHAPTER 6: RESEARCH METHODOLOGY

6.1 Introduction

This chapter aims to detail the research design and methodology of this study. To achieve this, the chapter begins by outlining the ontology, epistemology, methodology and axiology of the paradigm used for investigation into the research problem. Next, an overview of the research method used in this study is provided. Following this, the research strategy is discussed, which includes the experiment procedure and the online tools used in this experiment. Then, the data analysis methods used in this study are discussed. This is followed by an indication of the participants used in this study, which includes an overview of the broad context of the participants in this study. Finally, the evaluation criteria for the research is discussed and the ethical considerations pertaining to the study are outlined.

This study was conducted to explore how awareness, attitude and subjective norms influence the cost-benefit analysis users conduct. The purpose of this research was to review the factors that influence a user to disclose personal information online and investigate how an increase in awareness of the value of personal information could influence a user to safeguard their personal information. As such, the study creates a model that demonstrates how awareness, attitudes, and social norms influences a user's perception of the risks and benefits associated with information disclosure online.

6.2 Research Design

The research design describes the strategy selected to integrate the different research processes of the study in a clear and logical way to ensure the research problem is successfully addressed (Kirshenblatt-Gimblett, 2006). The structure of this chapter is informed by the components circled in orange in the research onion in figure 6.1. The research onion moves from the outermost layer to the core and depicts the "choice of data collection techniques and analysis procedures" (Saunders, et al., 2016, p. 122).

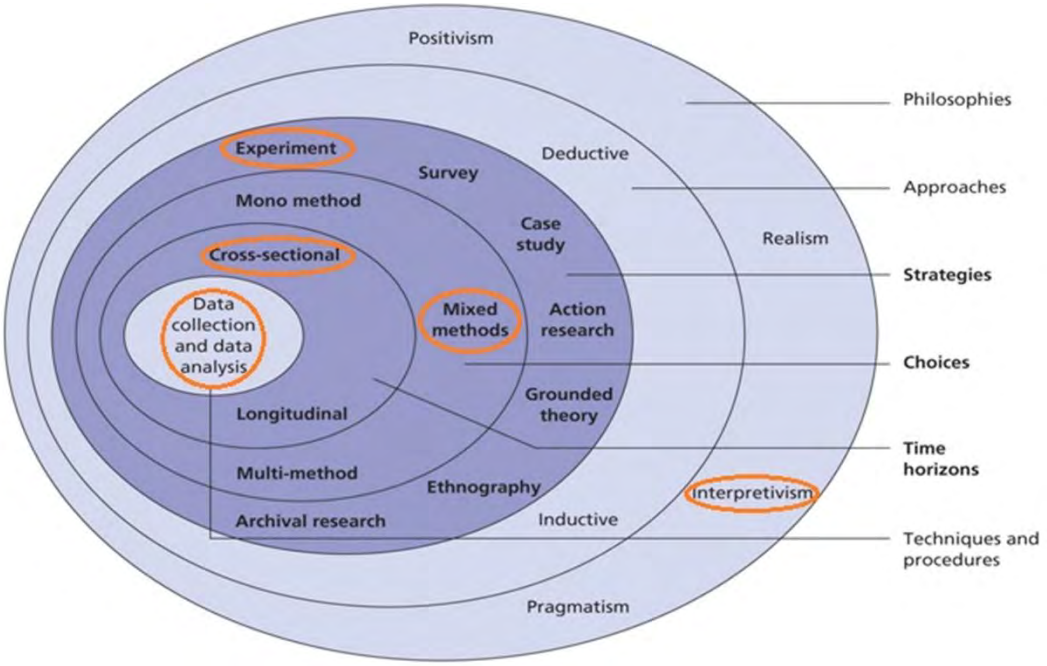


Figure 6.1 Research Onion adapted from Saunders, Lewis & Thornhill (2009)

6.2.1 Research Paradigm

The research paradigm significantly informs the design of a study and as such determines the questions asked, the data collected, and the interpretation of results (Bergman, 2010). Paradigms have been defined in many ways but overall, they refer to a worldview that is made up of assumptions and beliefs regarding knowledge that guide enquiry (Creswell & Clark., 2011). As seen in figure 6.1 the most common paradigms are positivism, realism, interpretivism and pragmatism. While the different paradigms have differing worldviews, they all discuss the elements of ontology, epistemology, axiology, methodology and rhetoric (Creswell & Clark., 2011). This study explored the research problem using the interpretivist paradigm because the researcher was striving to understand what drives a user's intention to disclose personal information online. As such, each element below is discussed in relation to this paradigm.

6.2.1.1 Interpretivism

Interpretive researchers consider reality to consist of people's understanding and interpretation of their experiences in the world. Thus, different people with different backgrounds can infer different meanings to the same social phenomena and therefore experience different social realities (Saunders, et al., 2016). As such, interpretivism argues that the methods used to study physical phenomena cannot be used to study the social worlds

of people because people interpret their world and act accordingly (Saunders, et al., 2016). Furthermore, the essence of interpretivism is to reconstruct and understand the existing subjective meanings of the social world in order to use them as stepping stones for theorizing without distorting their meaning (Goldkuhl, 2012). This is done by relying as much as possible on the participant's view of what is being studied (Creswell, et al., 2006). The interpretivist paradigm is best suited to this research, as the aim of this study is to understand and explore personal information disclosure online and to achieve this the researcher relies heavily on the views of participants who engage online regularly.

6.2.1.2 Ontology

Ontology refers to the nature of reality when researchers conduct their studies (Creswell & Clark., 2011). Interpretivist research adopts a relativist ontology where a phenomenon can have multiple interpretations that are based on different personal backgrounds and experiences (Shah & Al-Bargi, 2013; Kivunja & Kuyini, 2017). Consequently, interpretivists believe that reality is socially constructed through the individual's interaction with the world and others (Goldkuhl, 2012; Shah & Al-Bargi, 2013; McChesney & Aldridge, 2019). This type of ontology is particularly significant in this study because past experiences, values and background influenced how participants engaged online and freely the disclosed personal information.

6.2.1.3 Epistemology

Epistemology refers to how the researcher gains knowledge of reality (Creswell & Clark., 2011; Kivunja & Kuyini, 2017). This paradigm has a subjectivist epistemology where the researcher creates knowledge by interpreting the data collected using their own frame of reference and cognitive processing (Kivunja & Kuyini, 2017). Furthermore, when conducting the study, the researcher and subjects participate in a collaborative process where they engage in an open dialogue that allows both parties to listen, question, read and write (Kivunja & Kuyini, 2017). As a result, the researcher and the participants are both interpreters and creators of useful data. Thus, for the research to be effective it is essential that the interpretivist researcher "adopt an empathetic stance" (Saunders, et al., 2016, p. 141). In relation to this study the researcher and participants engaged in this collaborative process during the interview, where certain aspects and topics were expanded upon and unpacked to better understand the disclosure of personal information online.

Additionally, the foundation of interpretive research relies on providing a complete understanding of the research situation (Goldkuhl, 2012). To accomplish this, the researcher must provide an overview of the historical and social context of the study and its participants (Goldkuhl, 2012). This is because the results of interpretivist research are contextual understandings of a specific situation or phenomenon (McChesney & Aldridge, 2019).

6.2.1.4 Methodology

The interpretive methodology seeks to understand the world based on the social and historical perspectives of individuals (Creswell, 2009). Thus, researchers largely make use of qualitative research methods that place the emphasis on people as the principal research instrument (Creswell, 2009; Kivunja & Kuyini, 2017). This process is mostly inductive, as the researcher generates an understanding of the situation being researched by interpreting the data gathered in the field (Creswell, 2009).

While qualitative research methods are typically linked to the interpretivist paradigm a mixed-methods approach can also be applied to interpretivist research. According to Saunders, et al. (2016) and Creswell, et al. (2006), it is possible to conduct a mixed-methods study using an interpretive theoretical lens. This is because the association between a specific paradigm and research method is neither necessary nor sacred (Johnson & Onwuegbuzie, 2004). Thus, a single predominant paradigm such as interpretivism can be used for both the qualitative and quantitative aspects of a mixed-methods study (McChesney & Aldridge, 2019). To accomplish this the focus of the research must reflect the core interpretivist principle of understanding over generalising or critiquing (McChesney & Aldridge, 2019). This study employs a mixed method approach due to the complex nature of personal information disclosure online despite potential privacy risks. By adopting this approach, the researcher was able to integrate qualitative and quantitative findings to gain a holistic understanding of online information disclosure.

6.2.1.5 Axiology

Axiology refers to the role values play in the research process (Creswell & Clark., 2011). Interpretivist research has a balanced axiology which supposes that the research outcomes and contributions will display the researcher's values while simultaneously trying to present a balanced account of the findings (Kivunja & Kuyini, 2017). Thus, the interpretivist

researcher's own frame of reference plays a significant role in the research process because they interpret the results from the study (Saunders, et al., 2016).

In summation, the interpretivist paradigm allows the researcher to both describe and understand events, people and objects in their social context. In doing so, interpretivists are able to provide an increased level of authentic information related to their research problem (Pham, 2018). Furthermore, because interpretivist researchers can conduct interactive interviews, they are able to prompt and investigate the participant's thoughts, values, perspectives and perceptions that would otherwise remain overlooked (Wellington & Szczerbinski, 2007). This allows for advanced insights that can be used to facilitate a better interpretation of the results. On the other hand, one can also note some disadvantages related to interpretivism. For instance, interpretivist research is hard to generalise due to the contextual nature of the results and it can be difficult to verify the usefulness and validity of the research contributions by using scientific methods (Pham, 2018). Furthermore, the researchers own frame of reference influences the study when they interpret the results which can result in bias (Kivunja & Kuyini, 2017). To assist in mitigating bias this study makes use of triangulation, discussed in section 6.2.6.

6.2.2 Research Method

There are three main research methods a study can employ: quantitative, qualitative and mixed methods (Creswell, 2009). On the one hand, quantitative research tests the relationship between variables numerically and analyses data using statistics (Saunders, et al., 2016). On the other hand, qualitative research is reliant on narrative data that is used to explore the meanings participants assign to a situation and leads to the development of "conceptual frameworks and theoretical contributions" (Saunders, et al., 2016, p. 168). Finally, the mixed methods approach incorporates aspects from both quantitative and qualitative approaches (Creswell, 2009). As such, these methods can be conceptualized as falling on a continuum with mixed methods in the middle (Creswell, 2009).

Additionally, the research method a study adopts is often dependent on the chosen research paradigm. The paradigm of this study is interpretivism, which prescribes a qualitative approach. However, in section 6.2.1.3 it is shown that a mixed-methods approach can be applied in interpretivist research. As such, this research employs a qualitative mixed-methods approach. In a qualitative mixed-method approach, the quantitative data collected

plays a supportive role to the qualitative data (Creswell, et al., 2006). Thus, it is the qualitative data's responsibility to support and illustrate the qualitative results.

6.2.2.1 Mixed Methods

The mixed-methods approach to research can be seen as both a method and a methodology that involves gathering, examining and combining quantitative and qualitative approaches in a study (Creswell & Clark., 2011). At its core, mixed methods suggest that when a researcher combines statistical, quantitative data with qualitative data from the narratives of participants, a greater understanding of the research problem is provided (Creswell, 2014).

The different variations of mixed methods research designs are shown in figure 6.2. This study makes use of a concurrent mixed methods design where both qualitative and quantitative data can be used in support of one another to facilitate triangulation. In a concurrent design, qualitative and quantitative data is gathered in a single phase, which allows both sets of data to be interpreted at the same time (Saunders, et al., 2016).

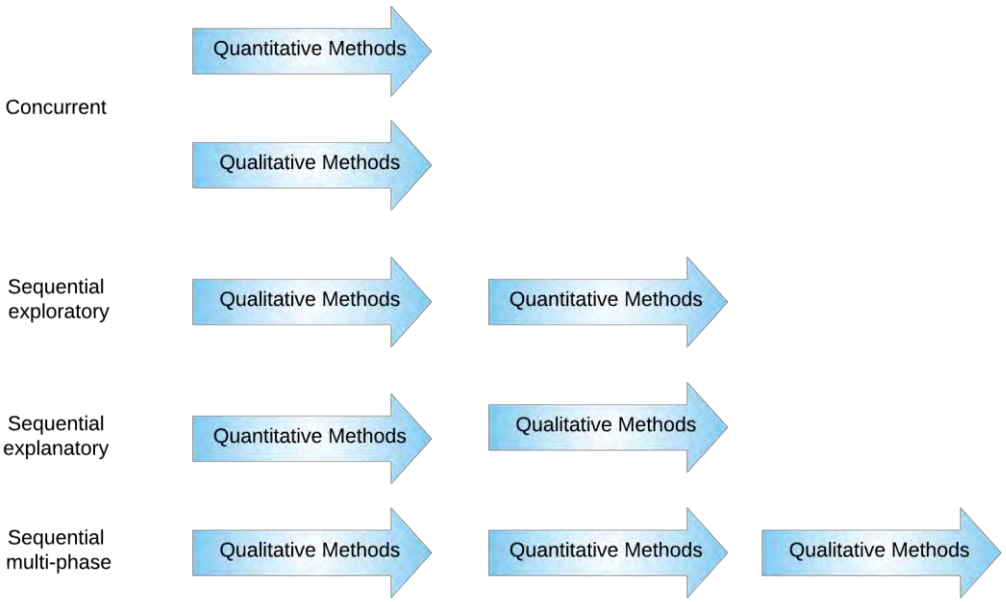


Figure 6.2 Mixed Methods Research Designs (Saunders, et al., 2016)

Overall, mixed methods add value to a study in various ways. For instance, using mixed methods increases the credibility of findings and assists in creating knowledge because findings can be triangulated (Hurmerinta-Peltomäki & Nummela, 2006; Creswell, 2014). Moreover, by adopting a qualitative mixed methods methodology it is possible to gain a

multi-layered view of social reality through deep listening that fosters more accurate descriptions of beliefs, attitudes and views (Hesse-Biber, 2010). This type of research method is useful for this project because understanding continued information disclosure online despite privacy risks is challenging and complex. Thus, by combining qualitative data and quantitative data an enhanced understanding of this behaviour can be achieved. Additionally, many studies in the area of self-disclosure on social media and online privacy solely focus on a quantitative approach. This use of a quantitative method can result in a shortfall that mixed methods can potentially address (McKim, 2017). Besides these reasons, in the context of Information Systems issues, a mixed-methods approach is well suited because these issues are multi-faceted and influenced by cultural, socio-technical and regional aspects (Peng, Nunes & Annansingh, 2011).

6.2.3 Research Strategy

This study utilizes a mixed-methods approach to explore how awareness, attitude and subjective norms influence the cost-benefit analysis users conduct in a single-phase experimental execution. To be more specific, a hybrid pre-experimental design is employed where a single group of participants are provided with an intervention during the experiment and no control group is used for comparison (Creswell, 2009). The following section details the experiment.

6.2.3.1 Experiment Procedure

Each participant completes a questionnaire to determine a baseline of the participant's initial disclosure intention. The participant was then instructed on how to download the personal data that Facebook, Google and Instagram stores about them. These instructions can be seen in Appendix B. Following the enactment of the GDPR in the EU, the right to access requires companies to provide users with the personal data stored about them once requested (Porter, 2019). The researcher then used various online tools detailed in section 6.2.3.2, to indicate the information publicly available about the user. Next, the results from the data requests and the findings from the tools were reviewed by the researcher and the participant via a semi-structured interview. Finally, the participant completed the questionnaire from step 1

again to potentially show an increase in their awareness and a change in their intention to disclose personal information. This process is illustrated in figure 6.3 below.

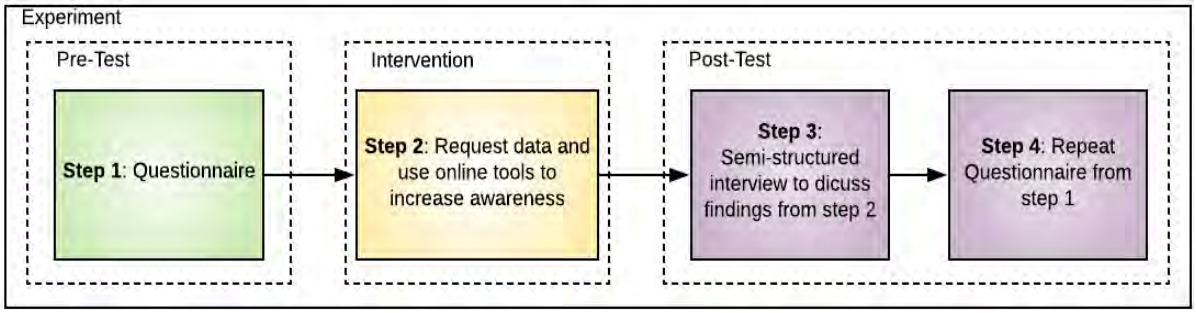


Figure 6.3 Data Collection Process

6.2.3.2 Online Tools

A few online tools are utilized in this study include Social Profile Checker, Facebook View As and HaveIBeenPawned. The Social Profile Checker by Salt. Agency is a free online tool that provides an overview of a user's digital footprint (Salt Agency, 2015). This tool uses Google and social media platforms to show users where they can be found online (Salt Agency, 2015). Next, the Facebook View As feature will be used to review what the participants publicly available profile looks like. This feature increases a user's awareness of what information appears on their public-facing profile and allows them to easily manage this information (Gartenberg, 2019). Finally, HaveIBeenPwned will be used to see if the participant's email account and any account associated with it has been involved in a data breach. The purpose of using HaveIBeenPwned is to determine whether a user's private information has been leaked (Hunt, 2013).

6.2.4 Data Collection and Analysis

As this study employs a mixed methods approach, both qualitative and quantitative data will be collected. The data collection and analysis methods used in this study are detailed in the following sub-sections.

6.2.4.1 Data Collection Method

The first data collection method used in this study was a questionnaire containing 40 questions exploring the participant's attitude, subjective norms, awareness, perceived benefits and perceived risks regarding information disclosure intention. These questions were based on both past studies examining online self-disclosure and questions developed by the researcher. Furthermore, the questionnaire was quantitative, containing Likert Type

Scale items based on a 4-point scale from Strongly Disagree to Strongly Agree. This scale was chosen because it is ipsative and thus forces a choice from the participant (Frey, 2018), which is useful when recording attitudes, perceptions and opinions.

The second data collection method used in this study was semi-structured interviews. In a semi-structured interview, some set questions or themes might be discussed, but the researcher has the freedom to tailor the interview to the participant by adding and omitting questions as needed (Saunders, et al., 2016). During the semi-structured interviews in this study, participants discussed their response to the data publicly available about them and their personal data stored by Facebook, Google and Instagram. Key questions for the interviews were related to similar topics as in the questionnaire such as awareness, attitude, behaviour and experience. Both the questionnaire and the interview schedule can be seen in Appendix C. A model showing the questions in the questionnaire that test the relationships in the model is also provided in Appendix C.

6.2.4.2 Data Analysis

In mixed methods research analysing data is referred to as mixed analysis, which involves using both qualitative and quantitative analytical techniques within the same study (Combs, 2011). In this study, descriptive statistics was the technique used to analyse the quantitative data from the questionnaires. Descriptive statistics enable the researcher to describe, compare and summarise the data collected (Fisher & Marshall, 2009; Saunders, et al., 2016). Furthermore, using descriptive statistics summarized data can be presented using visualizations such as pie charts, scatterplots and bar graphs (Wieringa, 2014). Thus, when combined with qualitative research, descriptive statistics allows the researcher to provide a more vivid picture of the phenomenon being studied (Schreiber, 2012).

To analyse the qualitative data from the semi-structured interviews, a thematic analysis was conducted. Thematic analysis refers to identifying and categorising data into appropriate codes to enable the discovery of themes or patterns in order to interpret different aspects of the research problem (Braun & Clarke, 2006; Rosala, 2019). This type of analysis is highly flexible and can provide a detailed account of data (Braun & Clarke, 2006). Furthermore, thematic analysis is useful for analysing the data in this study because it is suited to examining differing perspectives among participants (Braun & Clarke, 2006). In this study, the qualitative analysis software Nvivo 12 was used to determine important themes within the data based on the constructs in the Theory of Planned Behaviour and the Privacy

Calculus. Mind maps, treemaps and word clouds were created to visualize emerging themes, compare data and gain deeper insights from this data. The six phases of a thematic analysis outlined by Braun and Clarke (2006) that were followed in this study are summarized in figure 6.4.

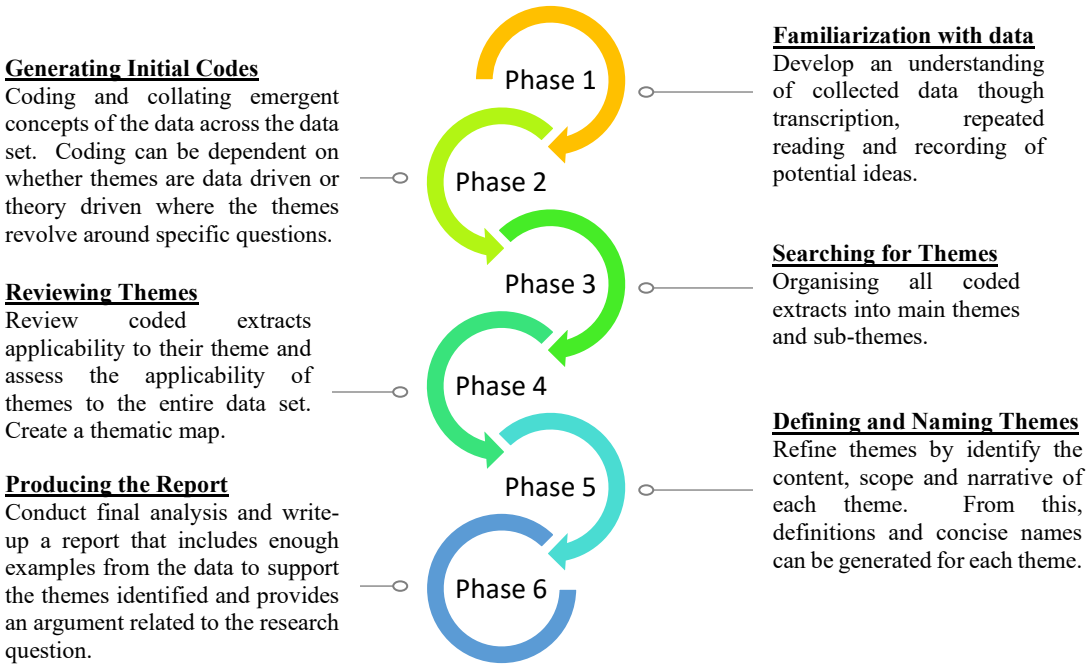


Figure 6.4 Phases of Thematic Analysis adapted from Braun and Clarke (2006)

The findings from the thematic analysis combined with the descriptive statistic provided the researcher with the ability to link the perceptions and opinions gathered regarding information disclosure intention and compare these with the quantitative responses from the questionnaire.

6.2.5 Participants

The experiment outlined in section 6.2.3.1 was conducted with fourteen Rhodes University students. This number was chosen because other qualitative studies that investigated aspects of online information disclosure used a sample size that ranged between eight and twenty participants (Lee, et al., 2013; Van Der Velden & El Emam, 2013; Krasnova, et al., 2010). In order to qualify, potential participants had to be active Facebook, Google and Instagram users, and between the age of 18 and 35 years old. This age range was chosen because the most frequent users of Facebook are between 18 and 40 years old (Contena, et al., 2015), while the most frequent users of Instagram are between 25 and 34 (Statistica, 2019). Participants were recruited via word of mouth and an advertisement posted on Facebook. The next section provides an overview of the broad context of the participants in this study to provide a complete understanding of the research situation.

6.2.5.1 Rhodes University Student Context

The participants in this study were students between 18 and 35 from Rhodes University in Grahamstown, South Africa. Furthermore, the participants in this study were from different faculties and departments in the University, with only a couple of students from the Information Systems Department. These students came from different socio-economic backgrounds and from both rural and urban settings (Rhodes University, 2015). In addition to this, at Rhodes University there is a mix of students from all over Southern Africa from government and private schools (Rhodes University, 2015). These students had varying religious backgrounds and therefore had different values and morals that influence their beliefs, attitudes and worldview. The common characteristic among these students is their "ability to achieve" (Rhodes University, 2015, p. 5). Furthermore, as university students they are deemed to have a higher-order of thinking that enables them to be creative, innovative and evaluative. The participants in this study grew up using technology, with Millennial students (aged 24-35) adopting social media early on as their main form of communication, while Generation Z students (aged 18-23) have "never known a world without social media" (Durfy, 2019). As such it is expected that they are computer literate and security conscious, but it must be noted that the participants might have different levels of competence when using technology and social media due to their exposure to these platforms. Overall, the social media mindsets of these two generational cohorts are different. Millennials are 'digital pioneers', who love to display their professional and personal lives

for all to see on Facebook and Instagram (Durfy, 2019). They are greatly influenced by their peers and are very susceptible to the Fear of Missing Out (Durfy, 2019). On the other hand, Generation Z's are true 'digital natives' because they have always had access to the Internet and social media (Durfy, 2019). They tend to be more private than millennials and use social media such as Instagram, Snapchat and YouTube, for entertainment rather than to show off their lives (Durfy, 2019).

6.2.6 Research Evaluation

To ensure the rigor and quality of the research, it is essential the researcher outlines how the study's findings were evaluated (Venkatesh, Brown, & Bala, 2013). As such, each of the researcher's choices should be justified and described (Stiles, 1999). In this study most methodological choices have been outlined in the previous sections, but a few points related to the evaluation of this research project remain.

Assessing the quality of research in a qualitative mixed methods study requires the use of alternative criteria (Saunders, et al., 2016) which in this case, include assessing the credibility, conformability, dependability, and transferability of the findings.

Credibility was achieved by allowing users to complete the same questionnaire once again after seeing the data collected about them by online platforms. By combining these questionnaires with the interview responses, the researcher was able to rule out alternative explanations and establish believable results that revolve around the participants holistic responses (Venkatesh, et al., 2013). Furthermore, completing two questionnaires acted as a form of participant validation, as participants were able to confirm and alter their responses if they wished in the second questionnaire. Participant validation refers to allowing participants to validate and confirm their responses (Saunders, et al., 2016). In this study credibility was also built through method triangulation. Method triangulation refers to using more than one method of collecting data, which is beneficial because it allows for more confidence in results (Lewis-Beck, et al., 2011). Thus, method triangulation assists in developing new ways to answer research questions and intensifies the richness of the findings (Peng, et al., 2011). The use of triangulation leads to an elimination of bias and error, leaving the truth to analyse (Mathison, 2011). In the context of this study, the results from the questionnaires and interviews were used to evaluate the proposed model seen in Chapter 5 section 5.2. This triangulation was also a tool to ensure conformability, which

refers the objectivity of the research during the data collection and analysis phases of the study (Mandal, 2018).

The next aspect to mention is dependability, which refers to recording and producing a reliable account of the research method and data (Saunders, et al., 2016; Mandal, 2018). To that end, the research method and procedure have been outlined in this chapter, while the results have been provided in Chapter 7. In relation to transferability, a detailed description of the context surrounding the participants was provided in the previous section. By providing this information the reader will be able to determine whether these findings can be applied in other settings (Mandal, 2018). As a final evaluation of the studies credibility and rigor it was condensed into journal articles and submitted to peer reviewed journals.

6.2.7 Ethical Considerations

Ethics assists researchers in determining how they should behave towards participants by stipulating what constitutes acceptable behaviour from a moral perspective (Vanclay, Baines & Taylor, 2013). The foundational ethical principles that need to be applied in research involving humans is respect for the research participant and informed consent (Vanclay, et al., 2013). As such, in all interactions with the participants the researcher demonstrated respect by recording their responses accurately and conducting the experiment in a polite and non-judgemental manner so as to facilitate a comfortable dialogue.

Furthermore, the researcher explained how the participant's information was used in terms of the study and ensured the participants signed a consent form allowing the use of their information. The participant invitation and consent form can be seen in Appendix D. Besides this consent, all participants were informed that they can withdraw at any time during the experiment and that participation was entirely voluntary. Moreover, all responses from the experiment remained anonymous and if any sensitive information was discovered about a participant during the experiment, this information was excluded from the study. The protection of the participant responses in the survey and interview was ensured by storing hard copies securely and limiting access to only the researcher and supervisor. Finally, ethical approval was obtained from Rhodes University's Ethics Committee of

Human Participants (clearance number 2020-0872-3206) before the experiment was conducted.

6.3 Summary

This chapter detailed the research design and methodology of this study. An interpretivist paradigm was chosen to explore the research problem, as the researcher was seeking to understand the factors that influence a user's intention to disclose. This paradigm adopts an interpretivist ontology where reality is socially constructed, a subjective epistemology where knowledge is jointly created by the researcher and participants, a methodology that emphasizes people as the main research instruments and a balanced epistemology where research results are influenced by the researcher's own frame of reference. A mixed methods approach was employed due to the complexity surrounding continued information disclosure online despite privacy risks. This approach allowed the researcher to gain a multi-layered view of this phenomenon by integrating qualitative and quantitative findings. To facilitate the mixed methods approach, an experiment was conducted where quantitative data was collected from Likert-scale questions in the questionnaire and qualitative data was collected during semi-structured interviews. This experiment was conducted with fourteen Rhodes University students, who were active Facebook, Google and Instagram users, and between the age of 18 and 35 years old. The resultant quantitative data from the experiment was analysed using descriptive statistics, while the analysis technique used for the qualitative data was thematic analysis. Finally, the entire experiment was informed by various ethical principles that the researcher followed including respecting the participant, ensuring the participant gave informed consent and was aware they can withdraw at any time. The next chapter will provide the analysis of the results obtained during the experiment.

CHAPTER 7: RESULTS

7.1 Introduction

This chapter presents the results from the mixed methods experiment conducted. The results from both the qualitative and quantitative aspects of the experiment are provided based on the construct they address. The results section begins by summarizing the demographic data of the sample to provide background on the context of the participants. Following this, results from the questionnaire and the identified themes are presented.

7.2 Mixed Methods Results

The responses from the questionnaire and the themes identified from the semi-structured interviews are combined to present the results of each construct identified in the model. The questionnaire included Likert Scale Items based on a 4-point scale from Strongly Disagree to Strongly Agree and items based on a 4-point scale from Very Risky to Very Useful. This scale was aimed at forcing participants to make a choice and as such slightly agree and strongly agree were combined to form agree, while slightly disagree and strongly disagree were combined to form disagree. Similarly, slightly and very risky were combined to form risky and slightly, and very useful were combined to form useful.

7.2.1 Participant Demographic Data

Of the fourteen participants in the study, seven (50%) were female, and seven (50%) were male. Furthermore, 50% of the sample were in the age range 18 to 23, and 50% were in the age range 24-35. Figure 7.1 below shows how much time participants reported spending on social media daily.

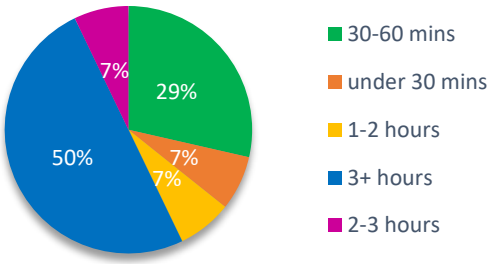


Figure 7.1 Daily Time Spent on Social Media

Figure 7.2 illustrates the number of friends and followers' participants have on Facebook and Instagram.

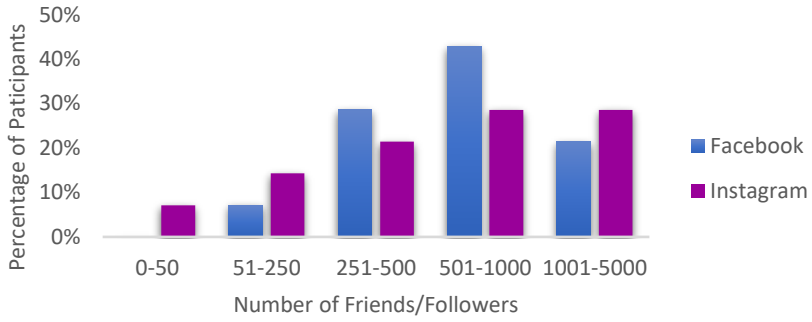


Figure 7.2 Number of Facebook Friends and Instagram Followers

Further analysis identified that 43% of participants have more Facebook friends than Instagram followers, 43% of participants have the same number of followers and friends on Facebook and Instagram, and only 14% reported having more Instagram followers than Facebook friends.

7.2.2 Attitude

The six items in the questionnaire related to attitude were aimed at evaluating how concerned participants were about their online privacy. Table 7.1 below provides a summary of the responses to these items before and after the experiment. From the data in this table one can see that following the experiment, a 14% decrease occurred in the number of participants who thought their data might be used in an unforeseen way. Furthermore, the experiment did not lower the percentage of participants who thought disclosing information was a good idea. However, a small increase was observed in relation to users believing disclosing and communicating personal information online is risky.

Additionally, the interview data highlighted a sense of concern regarding online privacy among most participants. 50% of participants had personally experienced privacy violations online, which affected their concern regarding the privacy of their information. Commenting on the effect of this incident on privacy concern, one participant stated: "After this incident, I really don't want people that I don't know to see my stuff" (Participant A). Besides personal privacy violations, a further 21% of participants mentioned they were affected by

the privacy violations of friends and family. Of these participants, only 14% engaged in privacy-protective measures.

Table 7.1 Summary of Responses to Attitude Items

Item	% Agree		% Disagree		Mean		Std. Deviation	
	Before	After	Before	After	Before	After	Before	After
I am concerned that Facebook and Instagram are collecting too much personal information about me.	86%	93%	14%	7%	3,14	3,64	0,66	0,63
I am concerned that the information I submit on Facebook, Google and Instagram can be used in a way I did not foresee.	100%	86%	0%	14%	3,64	3,64	0,50	0,74
It is desirable to protect my personal information on Facebook, Google and Instagram.	93%	100%	7%	0%	3,79	4,00	0,58	0,00
Disclosing personal information online is a good idea.	36%	36%	64%	64%	2,00	1,93	1,04	0,92
	% Useful		% Risky		Mean		Std. Deviation	
I think that giving information on Facebook, Google and Instagram that identifies me is:	21%	14%	79%	86%	2,07	1,64	0,62	0,74
I think that communicating personal information on Facebook and Instagram is:	36%	21%	64%	79%	2,07	1,57	1,00	0,85

Moreover, opinions differed regarding data being sent and stored off-shore. Over half of the participants (57%) did not mind if their data was stored off-shore provided the data was not being shared with third parties. A further 36% of participants said they do mind that their data is stored off-shore but feel they have no control over this aspect and 7% were indifferent. As one participant put it: “It is what it is if you want to access the service, you have to acknowledge that it is not a South African company” (Participant M). Finally, the majority of participants (64%) felt that online privacy was important, and as a result, they regulate the content they share. On the other hand, a more relaxed attitude towards privacy emerged among 36% participants. These participants felt that online privacy should be a concern, but because there are no physical threats, it is a concern for the future. For example, one participant stated: “I don’t really see the importance of online privacy yet because I have never had a situation where my account has been hacked or breached” (Participant P).

Another commented, “It is important but not really for everyday use, it is mainly for future use” (Participant H).

The theme of apathy towards privacy also emerged during the interviews, with 79% of participants. These views surfaced mainly concerning feeling ill-equipped to protect the information shared online and feeling a lack of control over what data is stored. Commenting on these issues, one participant said: “I have been safe in the things I do online and to realize that those things are taken and contribute to a profile. I now feel like I can’t do anything” (Participant O). Other issues mentioned include feeling unable to stop using social media and feeling privacy violations are inevitable. One participant argued that they expect social media platforms to store personal data about their users (Participant I). Another participant, speaking about unwelcome messages received from strangers, said:

> “Honestly [reporting] it does not make much of a difference because there are so many people sending dodge images and messages. It has become so normalized that this kind of thing happens”. (Participant L)

7.2.3 Trust in Social Media Provider

The objective of the three questions related to this construct was to determine whether participants feel a sense of trust towards social media platforms. A summary of the responses to these questions is provided in Table 7.2.

Table 7.2 Summary of Responses to Trust in Social Media Provider Items

Item	% Agree		% Disagree		Mean		Std. Deviation	
	Before	After	Before	After	Before	After	Before	After
Facebook, Google and Instagram are open and receptive to the needs of their members.	62%	50%	38%	50%	2,62	2,21	0,77	0,89
Facebook and Instagram make good-faith efforts to address most member concerns.	64%	50%	36%	50%	2,71	2,29	0,83	0,83
Online social networks are trustworthy.	21%	21%	79%	79%	1,79	1,64	0,80	0,84

The data in this table shows that following the experiment, the sample was equally divided in their opinions of whether these platforms are receptive to the needs of users and whether the platforms address member concerns. Furthermore, participants remained constant in

their opinion of whether social networks are trustworthy both before and after the experiment. From the response to this question, most participants do not believe social media platforms are trustworthy. Moreover, in the interviews, it emerged that participants are either sceptical or optimistic when it comes to whether online platforms protect the information of users. Almost two-thirds of the participants (64%) felt unsure whether online platforms protected their information. Commenting on this issue, one participant said: "I think from my perspective, looking at how easily I can find people's information they are not very good at protecting it" (Participant C). Some of these participants were also convinced that these platforms do not protect the information they provide. At the same time, 36% of participants felt these platforms do protect their information. For example, one participant said: "I think they do protect it because they stipulate that they do, but I think they still have lots of access to one's information" (Participant M). Additionally, 14% of these participants mentioned that because these platforms have privacy settings, they must be secure.

7.2.4 Subjective Norms

The three items related to subjective norms in the questionnaire were aimed at assessing whether important others in the participants life influence their risk and benefit perceptions. Table 7.3 provides a summary of the responses to the Likert Type Scale Items related to subjective norms before and after the experiment.

Table 7.3 Summary of Subjective Norms Likert Type Scale Items

Item	% Agree		% Disagree		Mean		Std. Deviation	
	Before	After	Before	After	Before	After	Before	After
People who are important to me think I should use Facebook, Instagram and Google because of the many benefits.	57%	57%	43%	43%	2,71	2,71	1,07	1,07
People who are important to me believe that I should be careful when exposing my information on Facebook, Instagram and Google.	79%	79%	21%	21%	3,21	3,21	0,97	0,97
	% Useful		% Risky		Mean		Std. Deviation	
People who are important to me believe communicating personal information on Facebook and Instagram is:	64%	64%	36%	36%	2,36	2.36	1,22	1,22

Closer inspection of the table illustrates that overall, participants felt important peers perceived more benefits to using social media. Furthermore, 29% of the participants suggested in the interview that not only do important peers influence one's perception of the benefits related to different platforms, but the academic institution also influences this perception.

Five broad themes emerged in relation to subjective norms in the semi-structured interviews. Many of these themes have overlapping content as they cover the influence of subjective norms on social media engagement. Figure 7.3 provides an illustration of the five themes identified and the prevalence of these themes amongst participants.

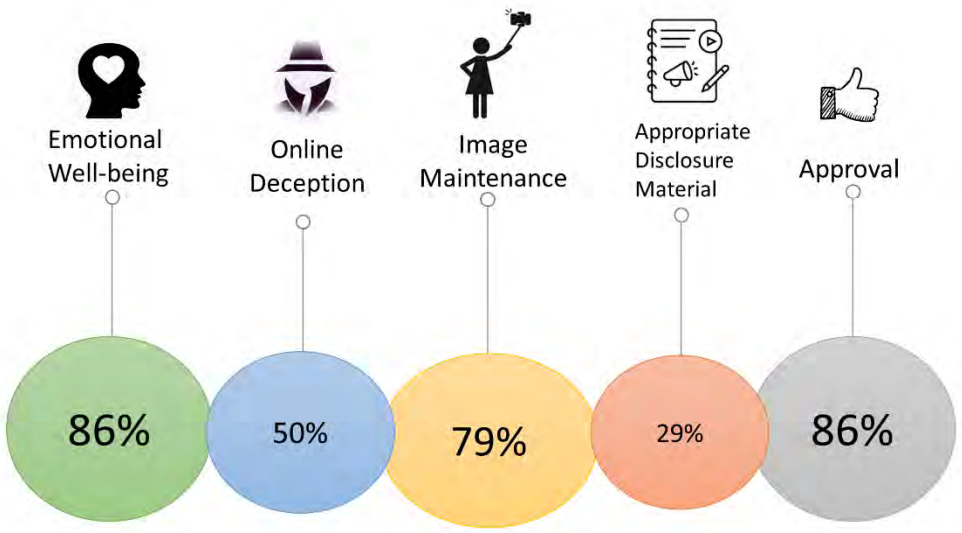


Figure 7.3 Prevalence of Themes Related to Subjective Norms

There was a sense among participants that engagement on social media affects their emotional well-being. 50% of participants reported that engaging on social media fosters a constant comparison to the prefect lives that others present online. Furthermore, the constant consumption of content that depicts friends and celebrities at their best lead to 43% of these participants either unfollowing certain accounts or deleting their social media accounts altogether. One participant reported that the content she was consuming was bad for her mental health, which caused her to delete her accounts until she had more control over regulating the amount of time spent on social media (Participant O). The consumption of negative content also arose as an issue some participants felt caused them anxiety when engaging on social media. This content included triggering posts that aim to unsettle and

aggravate others, as well as posts that cause guilt or aimed to manipulate the reader. Moreover, 14% of participants mentioned feeling anxious due to potentially unwanted people having the ability to see their posts on social media. These included ex-partners, stalkers and disgruntled friends. Additionally, 14% of participants mentioned that feeling dependent on social media and losing time that could be spent on more pressing tasks caused them stress and anxiety.

Furthermore, the deceptive nature of online content was also identified by participants. For instance, 21% of participants mentioned that users often present a façade on social media. Commenting on whether one gets to know people on social media, one participant said: "To an extent, because people do not always represent themselves as they really are online" (Participant L). The deceptive nature of the perfect life aesthetic was identified by 29% of participant, this included mentioning that no posts are written about the struggles people face and mostly proud and positive moments are shared on social media. Talking about this issue, a participant said: "It's only a small perspective of one's life you put on social media" (Participant C). Another participant mentioned that social media can be misleading because even when you are having the worst day, you can still make it seem as though you are leading the most exciting life (Participant E).

Participants also felt pressure to maintain a certain image online, with 36% of participants believing they have to post repeatedly to maintain their social presence. One participant argued that there is pressure to post continuously online, and as such, it is easier to avoid posting altogether (Participant H). A further 29% of participants felt anxious regarding whether the pictures and captions they post meet the standards of the platform. One participant commented: "There is pressure for your captions to be funny and entertaining and for your images to provoke something" (Participant C). Finally, the influence of others on the importance of privacy and thus, your portrayal online was identified by 14% of participants, who mentioned their families were very sceptical and private online. These participants mentioned taking extra precautions online due to the influence of their parents. For example, one participant said: "I am private online mainly because of my parents, who are very online safety conscious" (Participant I).

Only a small number of participants mentioned that certain posts are implicitly discouraged. The 29% of participants who discussed appropriate disclosure material mentioned that one should not post content that is considered too personal such as hard times, break-ups, loss of employment and mental issues. Commenting on sharing and consuming content on social media, one participant said:

> "It's more acceptable to show you are going through a rough time through memes and humour. Even though people are sharing stuff about mental illness and depression, they hardly ever go into this stuff. There is this veneer over certain issues that censors people". (Participant L)

Finally, seeking approval emerged as a theme that motivates most interaction on social media. Participants felt anxiety regarding whether their content is appropriate and the majority of them felt judged about the content they shared online. Of these participants, 36% mentioned taking 50 or more photos and then only posting one photo that ticks all the boxes. Furthermore, 50% suggested they feel anxious about how many likes their posts receive or whether their pictures are good enough. One participant stated: "The only reason for posting is so that people can see it and like it" (Participant P). Whilst another argued that the purpose of using Instagram was to allow people to see your content so that they can like and comment (Participant B).

7.2.5 FOMO

These three items in the questionnaire intended to understand whether users experienced FOMO. Table 7.4 below provides a summary of the responses to these items before and after the experiment.

Table 7.4 Summary of FOMO Likert Type Scale Items

Item	% Agree		% Disagree		Mean		Std. Deviation	
	Before	After	Before	After	Before	After	Before	After
When I have a good time, it is important for me to share the details online (e.g. updating status).	36%	36%	64%	64%	2,50	2,50	1,02	1,02
I post regularly on social networks to keep up with my friends.	36%	36%	64%	64%	2,43	2,43	0,94	0,94
It bothers me when I find out my friends are having fun without me.	43%	43%	57%	57%	2,71	2,71	0,99	0,99

It is apparent from this table that only a few participants seem to be affected by FOMO. This is interesting because 71% of participants agreed they experienced FOMO online when they see posts of their friends engaging in fun activities without them during the interviews. The chart in Figure 7.3 highlights the number of participants that experienced FOMO online in relation to their age and gender.

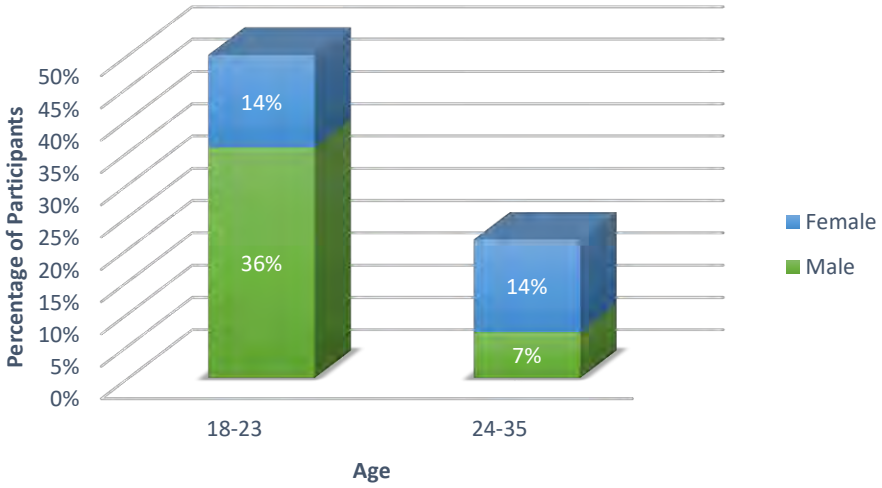


Figure 7.4 Age and Gender of Participants Experiencing FOMO

From this data, it appears that FOMO affects males more than females. The graph also shows that participants between 18 and 23 were more affected by FOMO. Of the 29% of participants that reported not experiencing FOMO 14 % said they used to experience FOMO when they were younger. For example, one participant said: "I used to experience FOMO, but it is not affecting me so much anymore" (Participant N). A minority of participants (21%) also indicated that experiencing FOMO is not something they like to admit. Additionally, 57% of participants reported that experiencing feelings of FOMO influenced them to post more frequently. One participant stated: "Sometimes after seeing my friend's posts, I do think I should be posting more because people should see that I am not just studying the whole time" (Participant I). Moreover, 50% indicated that they actively seek content to share online. Talking about this issue, a participant said:

> "I feel pressure to show I am also doing nice things. One time, I am not proud of it, I took a video my dad took in Russia of what was around him, and I posted it to pretend that it was me. I saw other people doing fun things, and I was just at home,

which really got to me so I posted the video and it got lots of attention". (Participant P)

7.2.6 Awareness

The objective of the four questions related to this construct was to determine whether participants were aware of the personal data stored by online platforms. A summary of the responses to these questions is provided in Table 7.5.

Table 7.5 Summary of Responses to Awareness Likert Type Items

Item	% Agree		% Disagree		Mean		Std. Deviation	
	Before	After	Before	After	Before	After	Before	After
I am aware that my Facebook and Instagram data can be sold to third parties, such as marketing or government agencies.	79%	93%	21%	7%	3,36	3,79	1,15	0,58
I follow news and the development of problems and violations concerning privacy.	86%	79%	14%	21%	3,00	3,00	0,96	1,04
I am aware that social media sites store personal data about me.	100%	100%	0%	0%	3,79	3,86	0,43	0,36
My knowledge of these privacy-related problems makes me believe that my personal information captured on Facebook, Instagram and Google is safe.	57%	29%	43%	71%	2,57	1,86	1,09	0,86

It is apparent from the table that participants were aware that social media sites store personal information about them. Furthermore, following the experiment, a 14% increase was apparent regarding being aware that data can be sold to third parties. In the interview, participants unanimously mentioned that they were unaware of the extent of data stored about them by online platforms. Besides being unaware of the amount of data stored, 36% of participants mentioned they did not know you were able to view the personal data stored by these platforms. A recurrent theme among participants was that they were ill-informed regarding the profiling done by Google and Facebook. 57 % of participants felt amazed by the detail and accuracy of the ad profiles created about them, while 21% of participants were upset by the inferences made, especially the marital status Google determined. Speaking about the profiling done by these platforms, one participant stated: "They can write a CV about me based on all this" (Participant N).

Additionally, a number of aspects were mentioned when asked about what surprised users most regarding the data collected. Figure 7.4 highlights the aspects participants found most surprising.

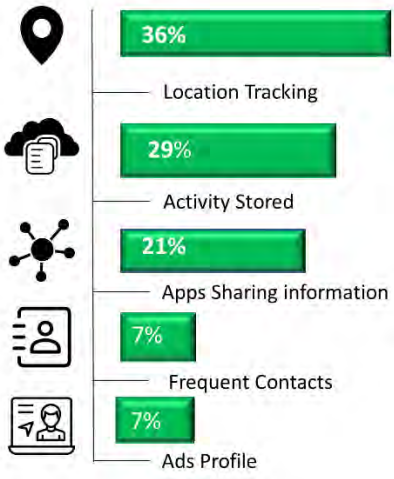


Figure 7.5 Participants Most Surprising Aspects of Data Stored

In this figure activity stored includes the search history and scope of activity, apps sharing information is apps that share offline information with Facebook and frequent contacts are based on emails and contacts shared with Google. Interestingly, while some users were shocked that their location was being tracked by Google, 29% of participants felt having their location tracked by Google was creepy but cool at the same time.

7.2.7 Personal Valuation of Information

To determine whether users attach personal value to their information, three questions were included in the questionnaire. The results from this section of the questionnaire are presented in Table 7.6.

Table 7.6 Summary of Responses to Personal Valuation of Information Questions

Item	% Agree		% Disagree		Mean		Std. Deviation	
	Before	After	Before	After	Before	After	Before	After
I am aware that my personal information is valuable.	93%	100%	7%	0%	3,64	3,86	0,84	0,36
I feel emotionally connected to my Facebook and Instagram profile and the information I share.	71%	71%	29%	29%	2,79	2,86	0,97	1,17
I protect my online data because it could potentially be sold to third parties.	64%	86%	36%	14%	2,86	3,29	1,10	0,91

From this data, one can see that all participants were aware that their personal information has value following the experiment. In the interviews, 50% of participants mentioned feeling more ownership and attachment to their data. For example, one participant remarked: "It is not just data, it is facets of your life. It is a reflection of one's self" (Participant B). This view was echoed by another participant who felt connected to their data because it was a reflection of their daily life and personality (Participant B). A small percentage of users (21%) felt that if their data were to disappear, they would not be upset. A further 14% of the participants felt no ownership over their data.

7.2.8 Perceived Risk

Four items in the questionnaire evaluated the participants perception of the risks involved when engaging online. The table below provides a breakdown of the responses to these items.

Table 7.7 Responses to Items Evaluating Perceived Risk

Item	% Agree		% Disagree		Mean		Std. Deviation	
	Before	After	Before	After	Before	After	Before	After
Overall, I see no real threat to my privacy due to my presence on social networks.	14%	14%	86%	86%	1,79	1,71	0,70	0,91
I fear that something unpleasant can happen to me due to my presence on social networks.	93%	79%	7%	21%	3,21	3,14	0,58	0,77
I am worried that unknown third parties will access my personal information from Facebook, Instagram and Google.	100%	86%	0%	14%	3,57	3,64	0,51	0,63
Potential risks to the privacy of my information online discourage me from disclosing information.	79%	86%	21%	14%	2,99	3,36	0,77	0,74

Interestingly, after seeing the information stored by these online platforms, a 14% decrease occurred in the number of participants who thought something unpleasant could happen to them due to their presence on social media. There was also a decrease in participants that were worried about third parties accessing their personal data. The interview also shed some light on risk perceptions, as following the experiment 50% of participants anticipated more risks to their information and 14% anticipated risks to their online network due to the information that is stored by Facebook, Google, and Instagram. One participant commented: "It is pretty easy for criminals to commit identity fraud if they gain access to all

this stored information" (Participant M). Another participant stated: "I am putting all my friends and family at risk, because if someone hacks into my account, then all their information is also available" (Participant I). Overall, the risks users anticipated included being stalked online, being kidnapped due to sharing location and online surveillance. A further 36% perceived more general risks such as being manipulated online and being judged. Additionally, only 29% of the participants had experienced repercussions from engagement on social media. These repercussions included unwanted attention following social media posts, feeling guilt or judgement after posting and feeling anxiety because unwanted people had access to posted content.

7.2.9 Perceived Benefits

The purpose of the five questions in this section of the questionnaire was to evaluate what benefits participants perceive when engaging online. The results obtained from the responses to these questions are set out in Table 7.8.

Table 7.8 Summary of Items Related to Perceived Benefits

Item	% Agree		% Disagree		Mean		Std. Deviation	
	Before	After	Before	After	Before	After	Before	After
Using online social networks is convenient to inform all my friends about my ongoing activities.	93%	86%	7%	14%	3,57	3,07	0,65	0,83
I believe sharing information online is positive and has many benefits.	93%	71%	7%	29%	3,07	2,79	0,73	0,80
I get to know new people through Facebook and Instagram.	86%	71%	14%	29%	3,07	2,79	0,76	1,07
I find Facebook, Google and Instagram entertaining.	100%	93%	0%	7%	3,79	3,57	0,43	0,85
I am willing to disclose personal information on Facebook, Instagram and Google because of the benefits I get from using these platforms.	57%	50%	43%	50%	2,57	2,43	0,94	1,02

Overall, these results show that following the experiment, some participants perceived less benefits related to engaging on social media. The overriding benefit of engagement on social media was for fun or entertainment with 100% agreement before the experiment and 93% agreement after the experiment. In the interviews, most participants agreed that the benefits of social media encourage them to disclose information, with only 21% disagreeing. A variety of perspectives were expressed regarding the benefits of using social media. This

included keeping up with friends, maintaining relationships, entertainment and using the platform as a tool for social change. For example, one participant argued that the Internet could be used to monitor societal issues such as gender-based violence and harassment in a more effective way (Participant L).

7.2.9.1 Intention

The final construct evaluated in the questionnaire was intention, which consisted of four questions. Only one of these questions appeared in both questionnaires, while the other three appeared only in the questionnaire following the experiment. Table 7.9 provides a summary of the results related to intention.

Table 7.9 Summary Responses to Intention Items

Item	% Agree		% Disagree		Mean		Std. Deviation	
	Before	After	Before	After	Before	After	Before	After
Overall, I am willing to reveal my personal information such as name, affiliation, etc.	71%	64%	29%	36%	2,86	2,64	1,03	1,08
I intend to continue using Facebook rather than discontinue its use.		79%		21%		3,00		0,68
I intend to continue using Instagram rather than discontinue its use.		79%		21%		3,07		0,73
I intend to continue using Google rather than discontinue its use		93%		7%		3,21		0,80

It is apparent from this table that the percentage of users willing to reveal personal information online following the experiment decreased by 7%. Furthermore, most participants intended to continue using these platforms, especially Google. The interviews highlighted that most users had already taken some steps to protect their information. Concerning their intention following the experiment, 43% of the participants reported they would adjust their privacy settings and change their passwords, 21% intended to disclose less information online and 14% intended to start reading the terms and conditions of online services. One participant argued that they could not stop using Google because they need it for their studies, but they need to be more vigilant about their engagement (Participant E). Another commented, “I want to go and have a look at these platforms to see if there is anything I can do to make it more secure” (Participant G). These comments illustrate that

there is a sense among participants that they intend to take more responsibility when it comes to protecting their information online.

7.3 Summary

This chapter presented the quantitative and qualitative results from the experiment conducted. There was a sense of concern about privacy among participants. Yet, an apathetic attitude towards privacy also emerged. Moreover, engagement on social media seem to affect well-being and encouraged users to seek approval from others. Finally, it became apparent that an unawareness exists of the amount of data stored and the profiling done by platforms. These aspects all had various effects on the participant's perceptions of the risks and benefits of disclosure, as well as their intention to disclose. Therefore, the next chapter moves on to discuss and interpret these results in order to effectively understand online disclosure.

CHAPTER 8: FINDINGS AND DISCUSSION

8.1 Introduction

This chapter aims to discuss the results presented in Chapter 7 in relation to the propositions determined in Chapter 5. The chapter starts by determining the influence of attitude on a user's risk and benefit perception. Next, the factors that influence a user's attitude towards disclosure are identified. Following this, the influence of subjective norms on a user's risk and benefit perception is analysed. Then, the influence of awareness on information disclosure is discussed. Finally, these aspects are tied together in relation to disclosure decisions.

8.2 Discussion of the Results

This study sought to determine the influence of attitude, subjective norms and awareness on the cost-benefit analysis users conduct when disclosing personal information online. To facilitate this discussion, the propositions will be addressed.

8.2.1 Influence of Attitude on Risk and Benefit Perception

It was proposed that a user's attitude towards privacy will influence their perception regarding the risks and benefits involved when disclosing online. The interviews highlighted that most participants were concerned about their online privacy due to privacy violations. These same participants anticipated risks to either themselves or their network. Furthermore, following the experiment participants felt providing personal information online is risky and potential risks to their information discourage them from disclosing online. This indicates that participants with a more concerned or cautious attitude towards privacy perceived and anticipated more risks to their information. This finding is consistent with that of Gerber, et al (2018) as they concluded that users who have experienced a privacy violation have an increased risk perception. Furthermore, these results also broadly support the findings of Robison (2018), who determined that a higher level of anxiety due to risk perception leads to a negative attitude towards online disclosure. This concern fosters the anticipation of potential risks to their information, which influence users to regulate the information they post online. This involves not posting location details and not sharing information that is considered too personal.

On the other hand, participants with a more relaxed attitude towards privacy perceived risks as being general and removed from them currently. These risks were more abstract such as being manipulated and judged, while concerned users perceived specific risks such as being kidnapped or stalked online. A possible explanation why users with a more relaxed attitude perceive risks as more abstract and removed from themselves might be because they have more optimism bias.

With regards to the benefits of disclosure, the interviews revealed that participants perceived benefits that encouraged their engagement on social media. These benefits ranged from entertainment and relationship maintenance to facilitating social change. The results of this study did not show a relation between a more relaxed attitude and an increased perception of benefit, as even participants who were concerned about their privacy still agreed that they disclose information due to the benefits of social media. This outcome is contrary to that of Robinson (2018), who determined that perceiving benefits leads to a more positive attitude towards disclosure. Furthermore, following the experiment, most participants felt that communicating personal information was risky, but they still intended to disclose and use social media sites.

These findings support previous studies that found evidence of the privacy paradox (e.g., Norberg, et al., 2007; Lee et al., 2013; Taddicken, 2014). A possible explanation why participants disclose online despite expressing concern regarding their privacy is that users regulate their disclosure by maintaining two spheres of privacy, one public and one private (Petronio, 1991). For instance, in this study, most participants had a Facebook account with more restricted privacy settings to communicate with family versus a public Instagram account to link to hashtags and share their content with known and unknown followers.

Moreover, this inconsistency between attitude and behaviour can be linked to the participants having a sense of apathy towards privacy, where they felt a lack of control over their information and an inability to protect their information online. This finding was also reported by Hargittai and Marwick (2016), who determined that participants are aware of the risks related to disclosure, but they are resigned to their lack of control over privacy violations. By having an apathetic attitude, the users in this study where able to disregard their concerns in order to use social media platforms to gain the benefits of engagement. This is consistent with Hoffmann, et al (2016) who posited that privacy cynicism allows users to engage online despite their concerns because they feel unable to control the

protection of their information. However, apathy did not stop participants from instituting protective measures over their information, rather participants either felt the little they did to protect their information was not enough. This accord with the observation of Hargittai and Marwick (2016) that even although users feel there is little regarding privacy violations, apathy does not cause users to cease instituting privacy-protective measures.

Taken together, these findings suggest that attitude towards disclosure influences risk perception as proposed, but benefit perception unexpectedly. Although a more relaxed attitude towards privacy did not affect benefit perception, an apathetic attitude allowed participants to discount their concern and continue engaging on social media to gain the benefits of use. This suggests that an overall apathetic attitude towards privacy can override the potential risks of disclosure. This supports the idea that attitude towards disclosure is established based on perceptions of the benefits and risks of disclosure, while overall attitude determines whether benefits will outweigh the risks in a given context (Li, 2012). These findings further provide insight into why users often make misinformed decisions regarding privacy, where contrary to the Privacy Calculus Theory users disclose information even when the risks are high, and the benefits are low.

8.2.2 Factors Influencing Attitude

The current study found that the main factor influencing attitude towards sharing personal information is past experience. To determine this, the researcher examined the insights gained from the 71% of participants who either experienced a privacy violation personally or were affected by privacy violations of family or friends and compared this to the data gathered in the questionnaire regarding concern for online privacy. The results indicate that personal privacy violations affected most participants concerned regarding the safety of their information, while second-hand experience momentarily motivated participants to engage in privacy-protective measures such as changing their password. This suggests that second-hand privacy violations could influence immediate privacy-protective behaviour but does not seem to have a long-term impact on privacy concern. These results reflect those of Gerber et al. (2018), who observed that users are more inclined to have a concerned attitude when they have personally experienced an online privacy violation than when their attitude towards privacy is based on second-hand experiences. Conversely, participants that did not experience privacy violation were far more relaxed regarding instituting privacy settings and

regulating posts. It seems possible that these users felt more confident when using social media because they had not experienced infringements. This observation is similarly expressed by Gómez-Barroso, et al. (2018), where users who have not experienced privacy violations are more confident online.

The second factor influencing attitude towards disclosure is trust towards the social media platform. The results of this study indicate that most participants do not believe social media platforms are trustworthy and are sceptical about their ability to protect disclosed information. The findings suggest that participants who were optimistic regarding the social media platforms ability to protect their data online had more a more relaxed attitude towards disclosure, whereas participants who were sceptical of social media platforms protection abilities had a more concerned attitude regarding disclosure. These findings are consistent with the literature, where trust in the social media platform has been seen to influence attitude towards disclosure (Heirman, et al., 2013; Chang & Heo, 2014; Bevan-Dye & Akpojivi, 2016). In general, these findings suggest that trust in the platform reduces concern and leads to a positive attitude.

The third factor that was found to influence attitude towards disclosure is perceived risk. The current study found that participants who perceived risks to their information felt more concerned. For instance, most participants feared something could happen to them because of their engagement on social media and were worried that third parties could access their information online. In accordance with the present results, previous studies have demonstrated that increased risk perceptions foster negative attitudes towards disclosure (Hajli & Lin, 2016; Gerber, et al., 2018; Robinson, 2018).

Finally, a user's personal valuation of their information was found to influence their attitude towards disclosure. The results of this study indicate that most participants feel a sense of ownership and emotional attachment to their online information. This is consistent with Spiekermann & Korunovska (2017), who concluded that through a sense of psychological ownership over their data users ascribe value to their data. These feelings of attachment and ownership urge users to protect their information because it represents facets of their lives and builds their online persona. Overall, an increased valuation of your information due to a sense of ownership and emotional attachment to their data facilitates increased concern about potential risks to this data and a more cautious attitude towards disclosure.

8.2.3 Influence of Subjective Norms on Risk and Benefit Perception

An objective of this study was to determine the influence of subjective norms on intention to disclose personal information online. Based on insights from the literature, it was proposed that subjective norms would influence a user's risk and benefit perception when disclosing information online. In relation to benefit perception in the questionnaire, the results indicate that most participants felt important peers perceived more benefits to using social media. There was also an indication that not only do peers influence the usage and benefit perception of certain platforms, but the university also has an influence because they require students to use specific platforms. These results are in agreement with Acquisti, et al. (2015), where it was concluded that users receive guidance from their environment and the people around them when they are uncertain about privacy.

The influence of others was found to determine how participants interact on social media platforms. These results were discovered during the interviews, where participants felt pressure to maintain their image online by posting appropriate and engaging content that match the norms of expression on the platform. Furthermore, some participants felt obligated to post content regularly enough to satisfy their peer's expectations. These results support the idea that users engage on social media to gain approval from their network. The likes and comments users receive on the content they post boost their self-esteem and make them feel appreciated by their peers. These findings are consistent with previous studies such as McLaughlin & Vitak (2012) and Gerber, et al., (2018) where it was observed that by following subjective norms of disclosure and engagement on social media platforms users are able to avoid social disapproval or sanction.

FOMO also plays a role in the benefits users perceive when using social media. The results from the questionnaire and interview indicate that FOMO affected most participants and generally caused them to actively seek content to post online. Due to their fear of missing out and potentially being socially isolated users try to prove they lead an exciting and fulfilling life in comparison to their network. In accordance with these findings, Jeong & Kim's (2017) demonstrated that the need to avoid social isolation in online platforms can override privacy concerns. Moreover, these findings suggest that FOMO enhances the effects of subjective norms on a user's disclosure behaviour. This is because FOMO encourages users to value the opinions of others more when engaging and disclosing on

social media. It is likely then that posting to relieve feelings of FOMO encourages disclosure and in turn allows users to gain the benefits of relationship building and entertainment.

On the other hand, no significant relation was found between subjective norms and risk perception. The influence of others on taking precautions such as instituting privacy settings due to the perception of potential risk only emerged among a small subset of participants. A possible explanation for this might be that instead of trying to conform to expectations of others regarding instituting privacy controls, participants were more influenced by the platform privacy norms. On Instagram the focus is on broadcasting your content to a large audience which requires a public profile, while Facebook allows a variety of privacy options to maintain relationships with friends and regulate disclosure to the general public. Consistent with this interpretation, on Instagram participants were equally divided between having public or private profile, while on Facebook all participants had reviewed or adjusted their privacy settings to regulate the disclosure to users both inside and outside their network. This finding is further corroborated by Shane-Simpson et al. (2018) who found participants who prefer using Twitter and Instagram were more likely to have public profiles, while users with privacy concerns tend to use Facebook because they can maintain a more private profile with known friends. Thus, the platforms privacy norms might influence user's to institute privacy controls or remain with the default settings.

It is also worth noting that participants felt their peers consider sharing personal information on social media useful rather than risky. A reason why participants perceived this might be because the purpose of social media is to connect with others through sharing content, thus peers will encourage disclosure to stay connected. Furthermore, the results indicate that participants do not disclose information that they consider too personal. This relates to the observation by Krämer & Schäwel (2020) that users have become skilled at disclosing in a way that increases benefits and minimises risks such as not disclosing too much intimate information online. Consequently, it seems that users manage their disclosure to align with their perception of what their peers expect while simultaneously not revealing details about their lives that might be too intimate or cast them in a negative light.

All in all, the combination of these findings suggest that subjective norms influence benefit perception, but not risk perception. The influence of peers did not significantly influence whether users perceived risks to their information. Instead, the privacy norms of the platform influenced protection intention. Enhanced by a fear of missing out and the need to

gain approval, subjective norms were found to drive disclosure and engagement on social media platforms. Previous studies confirm the influence of subjective norms on intention to disclose (e.g. Heirman, et al., 2013; Chang & Chen, 2014; Varnali & Toker, 2015). Thus, this finding lends support to the Theory of Planned Behaviour, where subjective norms directly influence intention to disclose information. However, the present study does raise the possibility that through the Fear of Missing Out the influence of subjective norms on intention to disclose is heightened and can override potential concerns. Furthermore, while it is unexpected that subjective norms do not influence risk perception, it seems plausible that the influence of others would have a greater impact on benefits perception because the nature of social media fosters disclosure to reap the reward of increased social contact and connection.

8.2.4 Awareness and Information Disclosure

The present study proposed that increased privacy awareness would reduce information disclosure online. Interestingly, many participants in this study were aware that social media sites stored personal information about them; however, they were unaware of the extent of their digital record on each platform. This finding is contrary to previous studies, which have suggested that users are unaware that online platforms collect and store information about them (Zlatolas, et al., 2015; Esteve, 2017). Moreover, following being made aware of the extent of personal data stored online, most participants realised their data can be sold to third parties, which is evident in the questionnaire results following being shown what information is available about them online. Participants were also unaware of the detailed inferences made about them by Google and Facebook to form an ads profile. Seeing the profiles created about them brought about concern regarding how these inferences are made and the usage of these profiles. These findings are further corroborated by Rader (2014) who found that awareness of inferences made based on this behavioural tracking was related to an increased level of concern. Overall, an awareness of the data stored by online platforms lead to most participants believing their data is unsafe online. Based on these findings, it is likely that a connection exists between awareness and risk perception. Thus, by increasing a user's awareness of the personal data stored about them, they can become more cognisant of potential threats to their data.

Furthermore, the results show that an increased awareness of the data stored by online platforms influences a user's personal valuation of information. Following being shown

what data is stored about them, all participants felt their personal information was valuable. This is in accordance with prior studies which have demonstrated that users perceive their data as having more value when it can potentially be breached or harvested (Spiekermann, et al., 2012; Spiekermann & Korunovska, 2017). Besides attaching more value to their data, the results indicate that feelings of ownership and attachment towards information increased following being shown what was stored. In turn, participants wanted more control and intended to regulating disclosure and adjusting privacy settings. Consequently, these findings suggest that an awareness of the value users place on their information might provide the motivation to protect their information online and regulate their disclosure. This idea matches previous observations that users who feel a sense of ownership over their information are motivated to protect it from potential loss or threat (Spiekermann & Korunovska, 2017; Millham & Atkin, 2018)

Collectively these findings suggest that increased awareness of the data collected by online platforms together with an understanding of the personal value users assign to their information leads to users wanting more control over their engagement on social media. Furthermore, these results support the replacement of perceived behavioural control with awareness in the social media context, as new insight may have emerged from evaluating the effects of awareness and personal valuation of information on disclosure intention. It can further be inferred that through privacy awareness, users are able to make informed decisions (Pötzsch, 2009). This is because an increased awareness of what is stored by online platforms allows users to become mindful of the value they assign to their data and the potential risks to this information, which in turn motivates them to institute privacy protective measures. The combination of these findings suggest that together both awareness and personal valuation of information can encourage users to protect their privacy and information online. Thus, becoming aware of personal data collection and the consequences of this, together with an understanding of the importance and value data has in the digital economy, is the first step towards empowerment (Becerril, 2018).

8.2.5 Effect of These Aspects on Information Disclosure

The model in Figure 8.1 depicts the factors that were found to influence risk and benefit perception. The model in Figure 8.2 highlights the between the conceptual model and final model

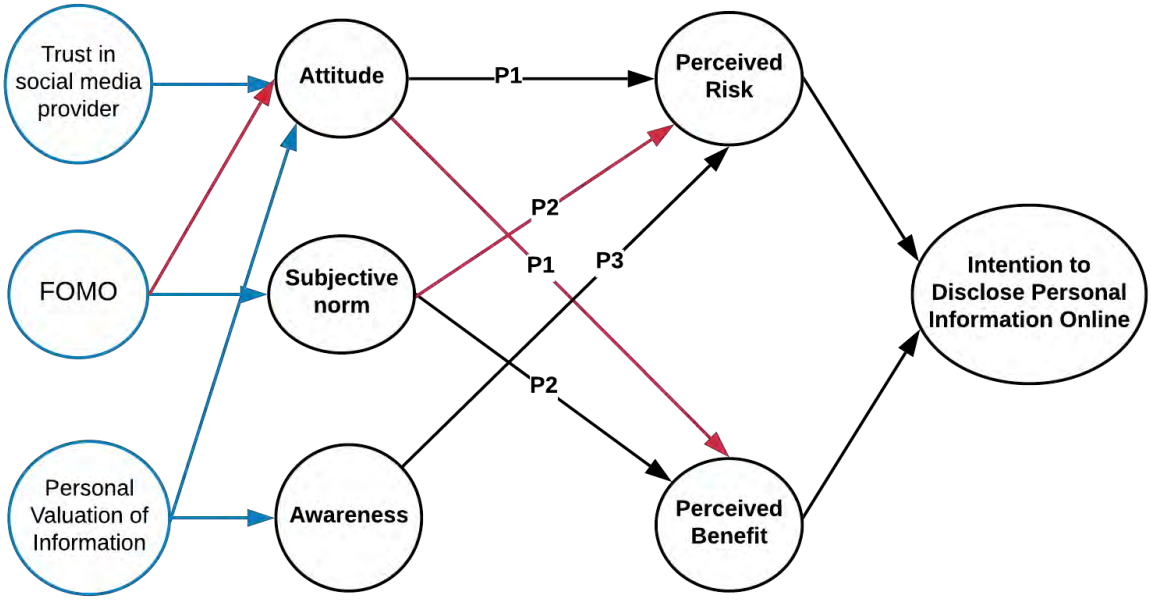


Figure 8.1 Conceptual Model Highlighting Changes

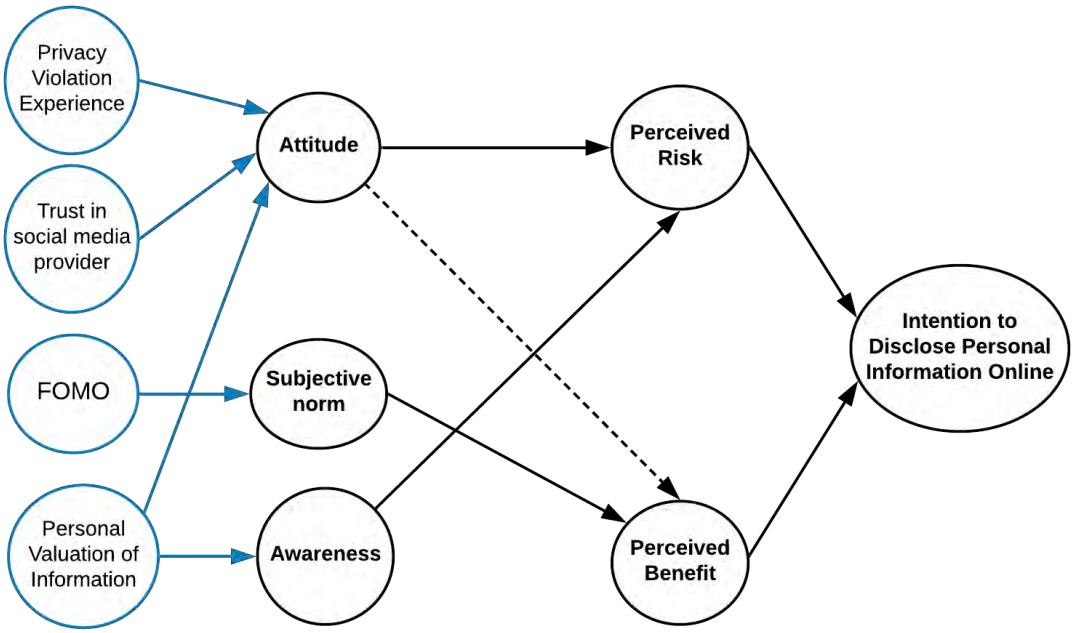


Figure 8.2 Final Influences on Information Disclosure Risk and Benefit Perception

The red arrows in Figure 8.1 represent the non-significant relationships that were removed. In Figure 8.2 attitude towards disclosure influences perceptions of risk, but not benefit. However, an overall apathetic attitude towards privacy allows users to disregard their privacy concerns to reap the benefits of disclosure. This apathetic attitude is illustrated by the dotted line leading to benefit perception. Additionally, the arrow between attitude and perceived risk is bidirectional because anticipating risks can foster a more cautious attitude toward disclosure. Privacy violation experience emerged as another factor that influences attitude.

To further understand the influence of these aspects on information disclosure the diagram in Figure 8.3 was created.

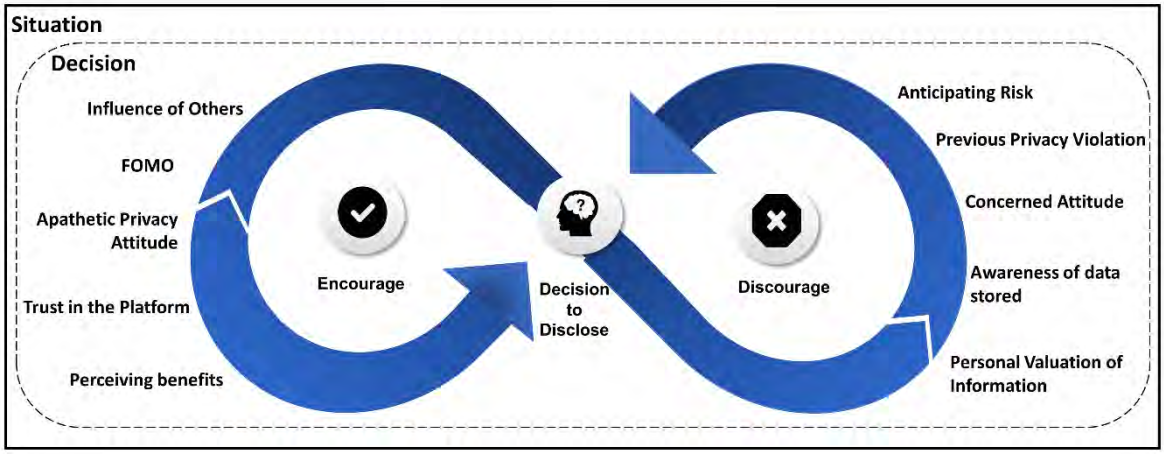


Figure 8.3 Factors That Encourage or Discourage Disclosure

The outside layer of the diagram depicts the context in which the privacy calculus is conducted. During the interviews, it became evident that decisions to disclose information are fluid and occur based on the context in which information is being requested. For instance, even participants who were concerned about their privacy were willing to reveal personal information such as contact information, address, and education information if they thought these details are necessary requirements to find potential employers and sponsors. This interpretation is supported by the idea that the privacy calculus has a situational nature, where each privacy decision is determined impulsively (Masur, 2019), dependent on the context in which the information is being disclosed. As a result, the aspects that encourage or discourage disclosure might fluctuate depending on the situation.

The inner layer of the diagram highlights the decision space, where the aspects identified either encourage or discourage disclosure. The two aspects that seem to most override potential risks and privacy concern are an apathetic privacy attitude and the perceived expectations of others. A resigned and apathetic attitude allows users to disregard their concerns in order to use social media platforms to gain the benefits of engagement. Furthermore, users seem strongly motivated to disclose and engage online based on their perception of what their network of friends and followers expected. Enhanced by FOMO, users are likely to value the perceptions and opinions of others over their own concerns. Thus, they disclose and engage online in ways that satisfy norms related to expression, appropriate content, and frequency of posting. This observation is consistent with Gerber, et al. (2018), where it was noted that social influences often affects actual behaviour over and above attitude. On the other hand, the main aspects that may discourage disclosure are previous privacy violations and an increased awareness of the personal value of information. Having first hand experienced a privacy violation leads to users being more concerned regarding the safety of their information and more cautious when engaging online. Finally, being cognisant of the personal value of information might encourage users to protect their information and regulate their disclosure online.

8.3 Summary

This chapter provided a discussion of the findings in relation to the propositions and theoretical framework of this study. Attitude and subjective norms were found to have interesting effects on risk and benefit perception. Furthermore, this study found promising results when replacing perceived behavioural control with awareness. In the context of online disclosure, combining awareness and personal valuation of information might act as a motivator for the protection of privacy online. The final chapter will summarize the findings and highlight the contribution of this study.

CHAPTER 9: CONCLUSION

9.1 Introduction

Social media has revolutionized the way people send and receive information by creating a new level of interconnected communication. However, while cyber-threats have increased and evolved, user awareness regarding these threats have not kept up the pace (Furnell & Moore, 2014). Besides these threats, the complex nature of privacy in an online context makes it hard for users to be completely aware of their extended network and the consequences of their disclosure.

The terms and conditions of companies like Google, Facebook and Instagram allow them to collect reams and reams of information on each user. This does not only include information users voluntarily shared, but also information collected about users through their online friends, which means even the most privacy conscious user is vulnerable (Bischoff, 2017). To make matters worse, since users often skip terms and conditions and privacy policies online, they are unaware of how their personal infromation is harvested, stored, processed and shared (Benson, et al., 2015; Steinfeld, 2016). This puts the power in the hands of the platform rather than the user.

This chapter provides an overview of the study in terms of the findings and their implications. The chapter starts by providing a summary of the research outcomes, which includes a synopsis of the research sub-questions in relation to the main research question. Next, the methodological approach of the study is discussed to provide a greater insight into how the study was conducted. Following this, the contribution of the study to both theory and practice is outlined. Finally, the limitations of the study and questions for future research are addressed.

9.2 Summary of Research Outcomes

Constant engagement and disclosure online can pose various threats to a user's personal data and online privacy. Users often remain unaware of the value of their personal information and continue to disclose excessively online despite potential risks to their privacy. As such, this study aimed to investigate what drives the disclosure of personal information online.

Prior research has found the Privacy Calculus to explain why users continue to disclose information online despite potential risks to their privacy (Gerber, et al., 2018; Krasnova, et al., 2010). However, this theory has come under scrutiny because it suggests that users determine whether to disclose based on a rational calculation of risks versus benefits.

To better understand the cost-benefit analysis user's conduct, this study integrated factors from the Theory of Planned Behaviour such as privacy attitude, subjective norms, and awareness with the Privacy Calculus.

Taking this problem background into account, the following main research question was developed:

> **How does awareness, attitudes, and subjective norms influence the cost-benefit analysis users conduct when deciding to disclose personal information online?**

In order to answer this main research question, five sub-questions were developed. Answers to these subquestions are summarised as follows:

a) *How does the Privacy Calculus influence information disclosure online?*
   The purpose of this question was to determine the influence of privacy calculus on information disclosure based on the literature surrounding self-disclosure on online platforms. This question was addressed in chapter 3, where the cornerstones of the privacy calculus were discussed. In sum, the Privacy Calculus Theory states that users weigh the cost of disclosure against the benefits, which determines their intention to disclose information (Culnan & Armstrong, 1999; Krasnova, et al., 2010). This suggests that people only disclose information when it will be beneficial to them in the long run.

   In this study, users perceived benefits to all engagement on social media and perceived risk when they had experienced previous privacy violations and had a greater awareness of the personal information stored about them by online platforms.

b) *How does attitude towards disclosure influence the cost-benefit analysis users conduct when disclosing information?* This question relates to the first proposition, which states that; *Attitude towards disclosure will influence a user's perception regarding the risks and benefits involved when disclosing online.* The investigation

into this proposition revealed interesting insights. Attitude towards disclosure was found to influence risk perception as proposed.

On the other hand, a carefree attitude towards disclosure did not affect benefit perception, but an apathetic attitude towards privacy allowed users to disregard their concerns about potential risks to their information to reap the rewards of disclosure on social media.

c) *What factors influence a user's attitude towards sharing personal information online?* The aim of this question was to determine the factors that influence a user's attitude towards disclosing personal information. It was found that having experienced online privacy violations was the main factor influencing attitude towards disclosure. Trust in the social media platform, perceived risk, and a user's personal valuation of their information were also found to influence attitude towards disclosure.

Overall, experiencing privacy violations, increased risk perception, and a user's increased personal valuation of their information foster a more concerned attitude towards disclosure, while trust in the platform leads to a positive attitude towards disclosure.

d) *How does subjective norms influence a user's intention to disclose personal information online?* This question relates to the second proposition, which states that; *Subjective norms influence a user's risk and benefit perception when disclosing information online.* The findings show that subjective norms only influence benefit perception. Moreover, subjective norms, amplified by FOMO, lead to users ignoring concerns and taking risks to satisfy the norms of expression and reciprocal sharing they believe their network of friends and followers expected.

Additionally, subjective norms were found to encourage disclosure because users are able to avoid social isolation and sanction by following the norms of engagement and expression on social media.

e) *How does information security awareness of the value of personal data influence perceived control over self-disclosure behaviour online?* This question relates to the third proposition, which states that; *Increased privacy awareness will reduce information disclosure online.* The investigation into the influence of awareness on information disclosure has shown that being aware of the personal data stored by online platforms increased the user's perception of the risks related to disclosure. Together, awareness of what is stored by online platforms and personal valuation of information can encourage users to protect their privacy and information online.

   Besides these findings, increased awareness of the data collected by online platforms and the personal value assigned to their information lead to users wanting more control over their engagement and disclosure on social media.

Overall, this research aimed to investigate what drives the disclosure of personal information online. To facilitate this investigation, the influence of attitude, subjective norms, and awareness on the cost-benefit analysis user's conduct was examined. Based on the findings in the previous section, it can be concluded that attitude, subjective norms, and awareness do influence a user's perception of either the risks and benefits involved when disclosing information online. The results indicate that subjective norms influence benefit perception, and awareness influences risk perception, while attitude influences both risk and benefit perception.

9.3 Methodological Approach

9.3.1 Experiment Procedure

This study explored the research problem using the interpretivist paradigm. An experiment was conducted using a mixed-methods approach to investigate how attitude, subjective norms, and awareness influence the cost-benefit analysis users conduct when making decisions.

Quantitative data was collected using a questionnaire containing Likert Type Scale items, which included questions based on both past studies examining online self-disclosure and self-developed questions. The qualitative data was collected in a semi-structured interview where participants discussed their response to the data publicly available about them and their personal data stored by Facebook, Google, and Instagram.

A recap of the experiment procedure is provided in Figure 9.1.

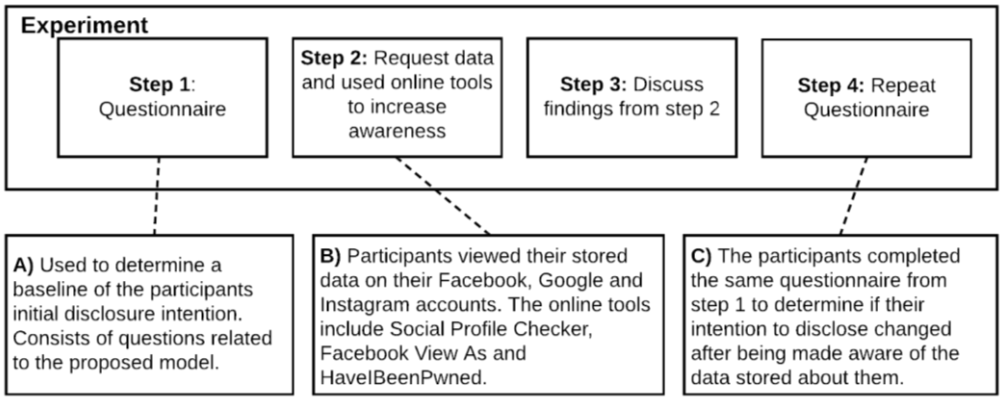


Figure 9.1 Experiment Procedure

The experiment was between 60 to 90-minutes long and was conducted with fourteen university students. In order to qualify, potential participants had to be active, Facebook, Google, and Instagram users, between the age of 18 and 35 years old.

9.3.2 Data Analysis

To analyse the qualitative data collected, a thematic analysis was conducted using the qualitative data analysis software, Nvivo 12, to determine important themes within the data. For each emerging theme, mind maps, tree maps, and word clouds were created to gain deeper insights and compare the data. Additionally, the quantitative data from the questionnaires were analysed using descriptive statistics. Together the findings from the qualitative and quantitative data provided more insight into information disclosure online.

9.4 Contribution of the Study

9.4.1 Contribution to Theory

This study contributes to theory by substituting the construct Perceived Behavioural Control with Awareness to align with a social media context. Furthermore, the study also extends to Theory of Planned Behaviour by adding *Trust in the Online Platform*, *FOMO* and *Personal Valuation of Information* as antecedent factors that influence *Attitude*, *Subjective Norms* and *Awareness*.

Additionally, this study also contributes theoretically by combining the Theory of Planned Behaviour and Privacy Calculus to account for social influences on the cost-benefit analysis users conduct when disclosing information online. To facilitate this, the constructs within

the Theory of Planned Behaviour serve as factors mediating the constructs in the Privacy Calculus Theory.

Overall, this study contributes to the understanding of privacy and information disclosure on social media among young people in South Africa. It adds to what is known about information disclosure online and provides a greater understanding of what influences a user's perception of the benefits and risks related to disclosing online. Specifically, the combination of the Theory of Planned Behaviour and the Privacy Calculus Theory attempts to account for privacy decisions often not being made through rational evaluation (Knijnenburg, et al., 2017; Wilson & Valacich, 2012). The addition of personal valuation of information, trust in the online platform, and FOMO as antecedent factors influencing disclosure has added to existing research by providing a more comprehensive evaluation of a user's intention to engage and disclose information online.

9.4.2 Contribution to Practice

The study also highlights that while users are conditioned to the fact that platforms are collecting and storing their data, actually seeing the extent of their online record makes them more aware of the value they assign to their information. Moreover, by providing an experiment that makes use of tools readily available to the public, the researcher is enabling users outside of the scope of the study to review their digital record on social media and other online platforms. This awareness of what is stored and the consequences of this data collection could provide users with the incentive to protect their privacy online and endeavour to be more responsible technology users.

9.5 Limitations of the Study

A limitation of this study is that it made use of a small sample size of only 14 participants. Thus, different findings might be discovered using a larger sample size. Furthermore, the sample population only consisted of students, which could potentially limit the generalizability of the findings.

Additionally, this study was conducted in South Africa, and thus diverse findings could occur in different countries. Thus, if the study was conducted elsewhere cultural differences might influence the impact of the identified factors on information disclosure online. Finally, the study only investigated intention to disclose personal information and not whether a user's actual behaviour changed following the experiment.

9.6 Future Research

Future research could focus on conducting the experiment in different contextual settings with larger sample sizes. Secondly, a fruitful area of future work might be to investigate the differences in gender when it comes to the influence of awareness, attitudes, and subjective norms on the cost-benefit analysis users conduct. Furthermore, a further study could explore whether users actually endeavour to institute measures to protect their information and regulate disclosure following the experiment.

Finally, a greater focus on an apathetic attitude towards privacy and how to alleviate the effects of this on information disclosure might produce interesting findings. In line with this, a stepping stone might be to determine ways in which users could actively protect their personal data online. This research could also analyse user awareness and knowledge of privacy settings.

9.7 Summary

This chapter has provided an overview of the most important aspects of this study. The summary of research outcomes highlighted that attitude, subjective norms, and awareness influence the cost-benefit analysis users conduct when disclosing information online. To gather the data used to produce these findings, a mixed-methods experiment was conducted. Furthermore, it was established that the study contributes to a broader understanding of privacy and information disclosure on social media. However, the study still has a few limitations and avenues for future research.

To conclude, this study has investigated information disclosure online from a holistic point of view. Hopefully, raising user awareness of what personal data is being stored and shared, might provide the wake-up call users need to acknowledge the risk, heed their privacy concerns and take responsibility for protecting their information online.

REFERENCES

Abel, J., Buff, C. & Burr, S., 2016. Social media and the fear of missing out: Scale development and assessment. *Journal of Business & Economics Research,* 14(1), pp. 33-44.

Abramova, O., Wagner, A., Krasnova, H. & Buxmann, P., 2017. Understanding Self-Disclosure on Social Networking Sites-A Literature Review. In *Proceedings of the 23rd Americas Conference on Information Systems*, (pp. 1-10). AIS.

Acquisti, A., & Gross, R. 2006. Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. In *Proceedings of the 6th International workshop on Privacy Enhancing Technologies*, (pp. 36-58). Springer.

Acquisti, A., Brandimarte, L. & Loewenstein, G., 2015. Privacy and human behavior in the age of information. *Science,* 347(6221), pp. 509-514.

Ajzen, I., 1991. The theory of planned behavior. *Organizational behavior and human decision processes,* 50(2), pp. 179-211.

Ajzen, I., 2002. Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior. *Journal of applied social psychology,* 32(4), pp. 665-683.

Ajzen, I., 2011. The theory of planned behaviour: Reactions and reflections. *Psychology & Health,* 26(9), p. 1113-1127.

Alashoor, T., & Al-Jabri, I. 2018. The Privacy Calculus under Positive and Negative Mood States. In *Proceedings of the 39th International Conference on Information Systems*, (pp. 1-17). AIS.

Ali, S., Rauf, A., Islam, N., Farman, H. and Khan, S., 2017. User Profiling: A Privacy Issue in Online Public Network. *Sindh University Research Journal,* 49(1), pp. 125-128.

Alkire, L., Pohlmann, J. & Barnett, W., 2019. Triggers and motivators of privacy protection behavior on Facebook. *Journal of Services Marketing,* 33(1), pp. 57-72.

Alqatawna, J., Madain, A., Ala'M, A. & Al-Sayyed, R., 2017. Online social networks security: Threats, attacks, and future directions. In: N. Taha, R. Al-Sayyed, J. Alqatawna & A. Rodan, eds. *Social Media Shaping e-Publishing and Academia.* Cham: Springer, pp. 121-132.

Ampong, G.O.A., Mensah, A., Adu, A.S.Y., Addae, J.A., Omoregie, O.K. and Ofori, K.S., 2018. Examining Self-Disclosure on Social Networking Sites: A Flow Theory and Privacy Perspective. *Behavioral Sciences,* 8(6), pp. 1-17.

Bandura, A., 1998. Health promotion from the perspective of social cognitive theory. *Psychology and health,* 13(4), pp. 623-649.

Bansal, G., Zahedi, F. & Gefen, D., 2010. The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision support systems,* 49(2), pp. 138-150.

REFERENCES

Barth, S. & De Jong, M., 2017. The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review. *Telematics and informatics,* 34(7), pp. 1038 - 1058.

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

Bauer, C., Korunovska, J., & Spiekermann, S. 2012. On the Value of Information: What Facebook Users are Willing to Pay. In: *Proceedings of the 20th European Conference on Information Systems*, (pp. 1-12). AIS.

Becerril, A., 2018. The value of our personal data in the Big Data and the Internet of all Things Era. *Advances in distributed computing and artificial intelligence Journal,* 7(2), pp. 71-80.

Benamati, J., Ozdemir, Z. & Smith, H., 2017. An empirical test of an antecedents–privacy concerns–outcomes model. *Journal of Information Science,* 43(5), pp. 583-600.

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), pp. 426-441.

Bregant, J. and Bregant, R., 2014. Cybercrime and computer crime. *The encyclopaedia of criminology and criminal justice*, pp.1-5.

Bergman, M., 2010. On concepts and paradigms in mixed methods research. *Journal of Mixed Methods Research,* 4(3), pp. 171-175.

Bevan-Dye, A. & Akpojivi, U., 2016. South African Generation Y students' self-disclosure on Facebook. *South African Journal of Psychology,* 46(1), pp. 114-129.

Beyens, I., Frison, E. & Eggermont, S., 2016. "I don't want to miss a thing": Adolescents' fear of missing out and its relationship to adolescents' social needs, Facebook use, and Facebook related stress. *Computers in Human Behavior,* 64, pp. 1-8.

Bischoff, P., 2017. *Comparing the privacy policy of internet giants side-by-side,* viewed 16 January 2020, Available at: https://www.comparitech.com/blog/vpn-privacy/we-compared-the-privacy-policies-of-internet-giants-side-by-side//

Blignaut, P., Burger, A., McDonald, T. & Tolmie, J., 2009. Computer attitude and anxiety. In: M. Khosrow-Pour, ed. *In Encyclopedia of Information Science and Technology.* 2nd ed. London: IGI Global., pp. 647-653.

Bol, N., Dienlin, T., Kruikemeier, S., Sax, M., Boerman, S.C., Strycharz, J., Helberger, N. & De Vreese C.H., 2018. Understanding the effects of personalization as a privacy calculus: Analyzing self-disclosure across health, news, and commerce contexts. *Journal of Computer-Mediated Communication,* 23, pp. 370-388.

Braun, V. & Clarke, V., 2006. Using thematic analysis in psychology. *Qualitative research in psychology,* 3(2), pp. 77-101.

Buglass, S., Binder, J., Betts, L. & Underwood, J., 2017. Motivators of online vulnerability: The impact of social network site use and FOMO. *Computers in Human Behavior,* 66, pp. 248-255.

Burns, S. & Roberts, L., 2013. Applying the theory of planned behaviour to predicting online safety behaviour. *Crime Prevention and Community Safety,* 15(1), pp. 48-64.

Cash, H., Rae, C. D., Steel, A. H. & Winkler, A., 2012. Internet Addiction: A Brief Summary of Research and Practice. *Current Psychiatry Reviews,* 8(4), p. 292–298.

Chaabane, A., Ding, Y., Dey, R., Kaafar, M.A. & Ross, K.W., 2014. *A closer look at third-party OSN applications: are they leaking your personal information?.* Cham , Springer, pp. 235-246.

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

Chang, C. & Heo, J., 2014. Visiting theories that predict college students' self-disclosure on Facebook. *Computers in Human Behavior,* 30, pp. 79-86.

Chang, S., Liu, A. & Shen, W., 2017. User trust in social networking services: A comparison of Facebook and LinkedIn. *Computers in Human Behavior,* 69, pp. 207-217.

Chang, Y., Wong, S. & Lee, H., 2015. Understanding Perceived Privacy: A Privacy Boundary Management Model. *In Proceedings of the 19th Pacific Asia Conference on Information Systems*, (pp. 1-13). AIS.

Cheikh-Ammar, M. & Barki, H., 2016. The influence of social presence, social exchange and feedback features on SNS continuous use: The Facebook context. *Journal of Organizational and End User Computing,* 28(2), pp. 33-52.

Chen, H.-T., 2018. Revisiting the privacy paradox on social media with an extended privacy calculus model: The effect of privacy concerns, privacy self-efficacy, and social capital on privacy management. *American behavioral scientist,* 62, pp. 1392-1412.

Cheung, C. M. K., Lee, Z. W. Y. & Chan, T. K. H., 2015. Self-disclosure in social networking sites: the role of perceived cost, perceived benefits and social influence. *Internet research,* 25(2), pp. 279-299.

Cho, H., Lee, J. & Chung, S., 2010. Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior,* 26(5), pp. 987-995.

Choi, B., Wu, Y., Yu, J. & Land, L., 2018. Love at first sight: The interplay between privacy dispositions and privacy calculus in online social connectivity management. *Journal of the Association for Information Systems,* 19(3), pp. 124-151.

Chon, B.S., Lee, J.K., Jeong, H., Park, J. and Park, J., 2018. Determinants of the Intention to Protect Personal Information among Facebook Users. *ETRI Journal,* 40(1), pp. 146-155.

REFERENCES

Cialdini, R. B. & Trost, M. R., 1988. Social influence: Social norms, conformity and compliance. In: D. Gilbert, S. Fiske & G. Lindzey, eds. *The handbook of social psychology.* 4th ed. New York: McGraw- Hill, pp. 151-192.

Cialdini, R.B., Demaine, L.J., Sagarin, B.J., Barrett, D.W., Rhoads, K. and Winter, P.L., 2006. Managing social norms for persuasive impact. *Social influence,* 1(1), pp. 3-15.

Combs, J., 2011. Data Analysis in Mixed Research: A Primer. *International Journal of Education,* 3(1), pp. 1-25.

Contena, B., Loscalzo, Y. & Taddei, S., 2015. Surfing on social network sites: A comprehensive instrument to evaluate online self-disclosure and related attitudes. *Computers in Human Behavior,* 49, pp. 30-37.

Creswell, J. W. & Clark., V. L. P., 2011. *Designing and Conducting Mixed Methods Research.* Thousand Oaks: SAGE.

Creswell, J., 2009. *Research design: Quantitative, qualitative and mixed methods.* Thousand Oaks: SAGE.

Creswell, J., 2014. *A Concise Introduction To Mixed Methods Research.* Thousand Oaks: SAGE.

Creswell, J., Shope, R., P. C. V. & Green, D., 2006. How interpretive qualitative research extends mixed methods research. *Research in the Schools,* 13(1), pp. 1-11.

Culnan, M. J. & Armstrong, P. K., 1999. Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science,* 10(1), pp. 104-115.

Debatin, B., Lovejoy, J., Horn, A. & Hughes, B., 2009. Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication,* 15(1), pp. 83-108.

Dhawan, S., Singh, K. & Goel, S., 2014. Impact of privacy attitude, concern and awareness on use of online social networking. In *Proceedings of the 5th International Conference-Confluence The Next Generation Information Technology Summit*, (pp. 14-17). IEEE.

Dienlin, T. & Metzger, M. J., 2016. An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative US sample. *Journal of Computer-Mediated Communication,* 21, pp. 368-383.

Dienlin, T. & Trepte, S., 2015. Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology,* 45(3), pp. 285-297.

Dinev, T. & Hart, P., 2006. An extended privacy calculus model for e-commerce transactions. *European Journal of Information,* 17(1), pp. 61-80.

REFERENCES

Dogan, V., 2019. Why Do People Experience the Fear of Missing Out (FOMO)? Exposing the Link Between the Self and the FoMO Through Self-Construal. *Journal of Cross-Cultural Psychology,* 50(4), pp. 524-538.

Douglas, R., 2020. *2020 Identity theft statistics,* viewed 10 January 2020, Available at: https://www.consumeraffairs.com/finance/identity-theft-statistics.html

Durfy, L., 2019. *Millennials vs Generation Z on Social Media,* viewed 2 December 2019, Available at: https://www.postbeyond.com/blog/millennials-genz-social-media/

Eadicicco, L., 2015. *The biggest difference between Google and Facebook — explained by someone who has worked at both,* viewed 15 January 2020, Available at: https://www.businessinsider.com/the-biggest-difference-between-google-and-facebook-2015-4?IR=T

Ellis, E., 2019. *Fighting Instagram's $1.3 Billion Problem—Fake Followers.* viewed 15 January 2020, Available at: https://www.wired.com/story/instagram-fake-followers/

Esteve, A., 2017. The business of personal data: Google, Facebook, and privacy issues in the EU and the USA. *International Data Privacy Law,* 7(1), pp. 36-47.

Facebook for Business, 2020. *Help your ads find the people who will love your business.* viewed 4 January 2020, Available at: https://web.facebook.com/business/ads/ad-targeting?_rdc=1&_rdr

Facebook, 2018. *Best practices for Facebook and Instagram,* viewed 22 December 2019, Available at: https://web.facebook.com/facebookmedia/blog/best-practices-for-facebook-and-instagram?_rdc=1&_rdr

Facebook, 2018. *Data Policy.* viewed 22 December 2019, Available at: https://web.facebook.com/policy.php?_rdc=1&_rdr

Farinosi, M. & Taipale, S., 2018. Who Can See My Stuff? Online Self-Disclosure and Gender Differences on Facebook. *Observatorio,* 12(1), pp. 53-71.

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, pp. 1-16.

Feng, B., Li, Q., Ji, Y., Guo, D. & Meng, X., 2019. Stopping the Cyberattack in the Early Stage: Assessing the Security Risks of Social Network Users. *Security and Communication Networks,* 2019, pp. 1-14.

Fisher, M. & Marshall, A., 2009. Understanding descriptive statistics. *Australian Critical Care,* 22, pp. 93-97.

Fogel, J. & Nehmad, E., 2009. Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior,* 25(1), pp. 153-160.

Fox, J. & Moreland, J., 2015. The dark side of social networking sites: An exploration of the relational and psychological stressors associated with Facebook use and affordances. *Computers in Human Behavior,* 45, pp. 168-176.

REFERENCES

Franchina, V., Vanden Abeele, M., Van Rooij, A.J., Lo Coco, G. & De Marez, L, 2018. Fear of missing out as a predictor of problematic social media use and phubbing behavior among Flemish adolescents. *International journal of environmental research and public health,* 15(10), pp. 2319-2336.

Frey, B., 2018. *The SAGE encyclopedia of educational research, measurement, and evaluation (Vols. 1-4).* Thousand Oaks : SAGE Publications.

Furnell, S. & Moore, L., 2014. Security literacy: the missing link in today's online society?. *Computer Fraud & Security,* 2014(5), pp. 12-18.

Garcia, D., 2017. Leaking privacy and shadow profiles in online social networks. *Science advances,* 3(8), pp. 1-6.

Gartenberg, C., 2019. *Facebook reenables 'View as Public' feature following 2018 security issue.* 15 January 2020, Available at: https://www.theverge.com/2019/5/14/18623445/facebook-view-as-public-feature-2018-security-issue-restored-back

Geber, S., Baumann, E., Czerwinski, F., & Klimmt C., The Effects of Social Norms Among Peer Groups on Risk Behavior: A Multilevel Approach to Differentiate Perceived and Collective Norms. *Communication Research*, doi: 10.1177/0093650218824213.

Gerber, N., Gerber, P. & Volkamer, M., 2018. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security,* 77, pp. 226-261.

Goldkuhl, G., 2012. Pragmatism vs interpretivism in qualitative information systems research. *European Journal of Information Systems,* 21(2), pp. 135-146.

Gollin, R., 2020. C*yber Threats Are Surging As Employees Work From Home Due To The COVID-19 Pandemic, Prompting Cybersecurity Insurers To Reassess Companies' Security Measures,* viewed 2 September 2020, Available at: https://www.mimecast.com/blog/the-impact-of-covid-19-on-cyber-security-insurance/

Gómez-Barroso, J., Feijóo, C. & Martínez-Martínez, I., 2018. Privacy calculus: Factors that influence the perception of benefit. *El profesional de la información,* 27(2), pp. 341-348.

Google Data Transparency, 2019. *Google Safety Centre.* viewed 3 January 2020, Available at: https://safety.google/privacy/data/

Google Privacy Policy, 2019. *Google Privacy & Terms.* viewed 3 January 2020, Available at: https://policies.google.com/privacy?hl=en-GB#infocollect

Google, 2020. *About.* viewed 3 January 2020, Available at: https://about.google/

Google, 2020. *AdSense Help.* viewed 3 January 2020, Available at: https://support.google.com/adsense/answer/140378?hl=en

Google, 2020. *Our Products.* viewed 4 January 2020, Available at: https://about.google/products/

Grandison, T. & Sloman, M., 2000. A survey of trust in internet applications. *IEEE Communications Surveys & Tutorials*, *3*(4), pp.2-16.

Guedes, E., Nardi, A.E., Guimarães, F.M.C.L., Machado, S. & King, A.L.S., 2016a. Social networking, a new online addiction: a review of Facebook and other addiction disorders. *MedicalExpress,* 3(1), pp. 1-6.

Guedes, E., Sancassiani, F., Carta, M.G., Campos, C., Machado, S., King, A.L.S. & Nardi, A.E.,2016b. Internet addiction and excessive social networks use: what about Facebook?. *Clinical Practice and Epidemiology in Mental Health,* 12(1), pp. 43-48.

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(11), pp. 11-123.

Han, M., Shen, S., Zhou, Y., Xu, Z., Miao, T. & Qi, J., 2019. An Analysis of the Cause of Privacy Paradox among SNS Users: take Chinese College Students as an Example. In *Proceedings of the 52nd Hawaii International Conference on System Sciences*, (pp. 6115-6124). AIS.

Hargittai, E. & Marwick, A., 2016. "What can I really do?" Explaining the privacy paradox with online apathy. *International Journal of Communication,* 10, p. 3737–3757.

Harkous, H., Fawaz, K., Lebret, R., Schaub, F., Shin, K.G., & Aberer, K., 2017. *AI Powered Privacy Policies.* viewed 3 January 2020, Available at: https://pribot.org/

Harkous, H., Fawaz, K., Lebret, R., Schaub, F., Shin, K.G., & Aberer, K., 2018. Polisis: Automated analysis and presentation of privacy policies using deep learning. In *Proceedings of the 27th USENIX Security Symposium*, (pp. 531-548). ACM.

Hasan, O., Habegger, B., Brunie, L., Bennani, N. and Damiani, E., 2013. A discussion of privacy challenges in user profiling with big data techniques: The EEXCESS use case. In *Proceedings of the 2013 IEEE International Conference on Big Data*, (pp.25-30). IEEE.

Hazari, S. & Brown, C., 2013. An empirical investigation of privacy awareness and concerns on social networking sites. *Journal of Information Privacy and Security,* 9(4), pp. 31-51.

Heaven, D., 2018. Your data, safe at last?. *New Scientist,* 238(3197), pp. 22-23.

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

Heravi, A., Mani, D., Choo, K. & Mubarak, S., 2017. Making Decisions about Self-Disclosure in Online Social Networks. In *Proceedings of the 50th Hawaii International Conference on System Sciences*, (pp. 1922-1931). AIS.

Heravi, A., Mubarak, S. & Choo, K., 2018. Information privacy in online social networks: uses and gratification perspective. *Computers in Human Behavior,* 84, pp. 441-459.

Hesse-Biber, S., 2010. Qualitative Approaches to Mixed Methods Practice. *Qualitative Inquiry,* 16(6), pp. 455-468.

Hoffmann, C., Lutz, C. & Ranzini, G., 2016. Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace,* 10(4).

Hofstra, B., Corten, R. & van Tubergen, F., 2016. Understanding the privacy behavior of adolescents on Facebook: The role of peers, popularity and trust. *Computers in Human Behavior,* 60, pp. 611-621.

Homans, G., 1958. Social behavior as exchange. *American journal of sociology,* 63(6), pp. 597-606.

Houser, K. & Voss, W., 2018. GDPR: The end of Google and Facebook or a New Paradigm in Data Privacy?. *Richmond Journal of Law & Technology,* 25, pp. 1-70.

Hoy, M. & Milne, G., 2010. Gender differences in privacy-related measures for young adult Facebook users. *Journal of Interactive Advertising,* 10(2), pp. 28-45.

Hu, Q. & Ma, S., 2010. Does Privacy Still Matter in the Era of Web 2.0? A Qualitative Study of User Behavior towards Online Social Networking Activities. In *Proceeding of the 14th Pacific Asia Conference on Information Systems,* (pp.591-602). AIS.

Hui, K.-L., Tan, B. & Goh, C., 2006. Online Information Disclosure: Motivators and measurements. *ACM Transactions on Internet Technology,* 6(4), pp. 415-441.

Hunt, T., 2013. *Who, what & why,* viewed 20 January 2020, Available at: https://haveibeenpwned.com/About

Hurmerinta-Peltomäki, L. & Nummela, N., 2006. Mixed methods in international business research: A value-added perspective. *Management International Review,* 46(4), pp. 439-459.

Ifinedo, P., 2012. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security,* 31(1), pp. 83-95.

Instagram, 2018. *Data Policy,* viewed 5 January 2020, Available at: https://help.instagram.com/155833707900388

Instgram, 2020. *Help Centre - Managing Your Account,* viewed 5 January 2020, Available at: https://help.instagram.com/173081309564229

Irshad, S. & Soomro, T., 2018. Identity Theft and Social Media. *Computer Science and Network Security,* 18(1) , pp. 43-55.

Ivana, 2018. *Online Profiling and The Risks,* viewed 5 January 2020, Available at: https://secureswissdata.com/online-profiling-and-the-risks/

Jafarkarimi, H., Saadatdoost, R., Sim, A. & Hee, J., 2016. Behavioral intention in social networking sites ethical dilemmas: An extended model based on Theory of Planned Behavior. *Computers in Human Behavior,* 62, pp. 545-561.

Jakovljević, M., 2011. Information Privacy: The Attitudes and Behaviours of Internet Users. *Oeconomica Jadertina,* 1(1), pp. 12-29.

Jeong, Y. & Kim, Y., 2017. Privacy concerns on social networking sites: Interplay among posting types, content, and audiences. *Computers in Human Behavior,* 69, pp. 302-310.

Jiang, Z., Heng, C. & Choi, B., 2013. Research note—privacy concerns and privacy-protective behavior in synchronous online social interactions. *Information Systems Research,* 24(3), pp. 579-595.

Johnson, R. B. & Onwuegbuzie, A., 2004. Mixed Methods Research: A Research Paradigm Whose Time has Come. *Educational Researcher,* 33(7), pp. 14-26.

Joinson, A., Reips, U., Buchanan, T. & Schofield, C., 2010. Privacy, trust, and self-disclosure online. *Human–Computer Interaction,* 25(1), pp. 1-24.

Junger, M., Montoya, L. & Overink, F., 2017. Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior,* 66, pp. 75-87.

Kang, R., Dabbish, L., Fruchter, N. & Kiesler, S., 2015. "My Data Just Goes Everywhere:" User mental models of the internet and implications for privacy and security, In *Proceedings of the 11th Symposium on Usable Privacy and Security*, (pp. 39-52). USENIX.

Kaushik, K., Jain, N. & Singh, A., 2018. Antecedents and outcomes of information privacy concerns: Role of subjective norm and social presence. *Electronic Commerce Research and Applications,* 32, pp. 57-68.

Kehr, F., Kowatsch, T., Wentzel, D. & Fleisch, E., 2015a. Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal,* 25(6), pp. 607-635.

Kehr, F., Wentzel, D. & Kowatsch, T., 2014. Privacy Paradox Revised: Pre-Existing Pre-Existing Attitudes, Psychological Ownership, and Actual Disclosure Privacy Paradox. In *Proceedings of the 35th International Conference on Information Systems*, (pp. 1-15). AIS.

Kehr, F., Wentzel, D., Kowatsch, T. & Fleisch, E., 2015b. *Rethinking Privacy Decisions: Pre-Existing Attitudes, PreExisting Emotional States, and a Situational Privacy Calculus. In Proceedings of the 23rd European Conference on Information Systems,* (pp. 1-15). AIS.

Kemp, S., 2020. *More Than Half Of The People On Earth Now Use Social Media,* viewed 2 September 2020, Available at: https://datareportal.com/reports/more-than-half-the-world-now-uses-social-media

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).

Kim, D., Park, K., Park, Y. & Ahn, J., 2019. Willingness to provide personal information: Perspective of privacy calculus in IoT services. *Computers in Human Behavior,* 92, pp. 273-281.

Kim, E., Lee, J., Sung, Y. & Choi, S., 2016. Predicting selfie-posting behavior on social networking sites: An extension of theory of planned behavior. *Computers in Human Behavior,* 62, pp. 116-123.

Kim, M. & Kim, S., 2018. Factors influencing willingness to provide personal information for personalized recommendations. *Computers in Human Behavior,* 88, pp. 143-152.

Kircaburun, K., Alhabash, S., Tosuntaş, Ş. & Griffiths, M., 2018. Uses and Gratifications of Problematic Social Media Use Among University Students: a Simultaneous Examination of the Big Five of Personality Traits, Social Media Platforms, and Social. *International Journal of Mental Health and Addiction,* pp. 1-23.

Kirshenblatt-Gimblett, B., 2006. *Part 1, what is research design? The context of design.,* 19 January 2020, Available at: http://www.nyu.edu/classes/bkg/methods/005847ch1.pdf

Kivunja, C. & Kuyini, A., 2017. Understanding and Applying Research Paradigms in Educational Contexts. *International Journal of higher education,* 6(5), pp. 26-41.

Knijnenburg, B., Raybourn, E., Cherry, D., Wilkinson, D., Sivakumar, S., & Sloan, H., 2017. Death to the Privacy Calculus? Available at SSRN: http://dx.doi.org/10.2139/ssrn.2923806

Kokolakis, S., 2017. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security,* 64, pp. 122-134.

Koohang, A., Paliszkiewicz, J. & Goluchowski, J., 2018. Social media privacy concerns: trusting beliefs and risk beliefs. *Industrial Management & Data Systems,* 118(6), pp. 1209-1228.

Koohikamali, M., Peak, D. & Prybutok, V., 2017. Beyond self-disclosure: Disclosure of information about others in social network sites. *Computers in Human Behavior,* 69, pp. 29-42.

Kordzadeh, N., Warren, J. & Seifi, A., 2016. Antecedents of privacy calculus components in virtual health communities. *International Journal of Information Management,* 36(5), pp. 724-734.

Koroleva, K., Brecht, F., Goebel, L. & Malinova, M., 2011. 'Generation Facebook' – A Cognitive Calculus Model of Teenage User Behavior on Social Network Sites. In *Proceedings of the 17th Americas Conference on Information Systems*, pp. 1-8. AIS.

Krämer, N. & Schäwel, J., 2020. Mastering the challenge of balancing self-disclosure and privacy in social media. *Current opinion in psychology,* 31, pp. 67-71.

Krasnova, H. & Veltri, N. F., 2011. Behind the curtains of privacy calculus on social networking sites: the study of Germany and the USA. In *Proceedings of the 10th International Conference on Wirtschaftsinformatik,* (pp. 891-900). Lulu.

Krasnova, H. & Veltri, N., 2010. Privacy calculus on social networking sites: Explorative evidence from Germany and USA. In *Proceedings of the 43rd Hawaii International Conference on System Sciences*, (pp. 1-10) IEEE.

Krasnova, H., Günther, O., Spiekermann, S. & Koroleva, K., 2009. Privacy concerns and identity in online social networks. *Identity in the Information Society,* 2(1), pp. 39-63.

Krasnova, H., Kolesnikova, E. & Günther, O., 2009. *It Won't Happen To Me!: Self-Disclosure in Online Social Networks.* In: Proceedings if the 15th Americas Conference on Information Systems, (pp 1-10). AIS.

Krasnova, H., Spiekermann, S., Koroleva, K. & Hildebrand, T., 2010. Online Social Networks: Why We Disclose. *Journal of Information Technology,* 25(2), pp. 109-125.

Krasnova, H., Veltri, N. & Günther, O., 2012. Self-disclosure and Privacy Calculus on Social Networking Sites: The Role of Culture. *Business & Information Systems Engineering,* 4(3), pp. 127-135.

Kroll, T. & Stieglitz, S., 2019. Digital nudging and privacy: improving decisions about self-disclosure in social networks. *Behaviour & Information Technology,* pp. 1-19.

Kumar, V. & Nanda, P., 2019. Social Media to Social Media Analytics: Ethical Challenges. *International Journal of Technoethics,* 10(2), pp. 57-70.

Lam, I., Chen, K. & Chen, L., 2008. *Involuntary information leakage in social network services.* Berlin, Springer, pp. 167-183.

Lambert, A., 2016. Intimacy and social capital on Facebook: Beyond the psychological perspective. *New Media & Society,* 18(11), pp. 1-17.

Laufer, R. & Wolfe, M., 1977. Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues,* 33(3), pp. 22-42.

Lee, H., Park, H. & Kim, J., 2013. Why do people share their context information on Social Network Services? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk. *International Journal of Human-Computer Studies,* 71(9), pp. 862-877.

Lewis-Beck, M., Bryman, A. & Liao, T. eds., 2011. Triangulation. In: *The SAGE Encyclopedia of Social Science Research Methods.* Thousand Oaks: Sage Publications, Inc.

Li, H., Luo, X., Zhang, J. & Xu, H., 2017. Resolving the privacy paradox: Toward a cognitive appraisal and emotion approach to online privacy behaviors. *Information & management,* 54(8), pp. 1012-1022.

Li, K., Wang, X., Li, K. & Che, J., 2016. Information privacy disclosure on social network sites: An empirical investigation from social exchange perspective. *Nankai Business Review International,* 7(3), pp. 282-300.

Li, Y., 2012. Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems,* 54(1), pp. 471-481.

Lin, W., Zhang, X., Song, H. & Omori, K., 2016. Health information seeking in the Web 2.0 age: Trust in social media, uncertainty reduction, and self-disclosure. *Computers in Human Behavior,* 56, pp. 289-294.

Lin, X., Featherman, M. & Sarker, S., 2017. Understanding factors affecting users' social networking site continuance: A gender difference perspective. *Information & Management,* 54(3), pp. 383-395.

Lindh, M. & Nolin, J., 2016. Information we collect: Surveillance and privacy in the implementation of Google Apps for Education. *European Educational Research Journal,* 15(6), pp. 644-663.

Liu, Z., Min, Q., Zhai, Q. & Smyth, R., 2016. Self-disclosure in Chinese micro-blogging: A social exchange theory perspective. *Information & Management,* 53(1), pp. 53-63.

Lo, J. & Riemenschneider, C., 2010. An Examination of Privacy Concerns and Trust Entities in Determining Willingness to Disclose Personal Information on a Social Networking Site. In *Proceeding of the 16th Americas Confernces on Information System,* (pp. 1-11). AIS.

Loiacono, E., 2015. Self-disclosure behavior on social networking web sites. *International Journal of Electronic Commerce,* 19(2), pp. 66-94.

Lowry, P., 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), pp. 163-200.

Lutz, C., Hoffmann, C., Bucher, E. & Fieseler, C., 2018. The role of privacy concerns in the sharing economy. *Information Communication & Society,* 21(10), pp. 1472-1492.

Mahmoodi, J., Čurdová, J., Henking, C., Kunz, M., Matić, K., Mohr, P. & Vovko, M., 2018. Internet users' valuation of enhanced data protection on social media: Which aspects of privacy are worth the most?. *Frontiers in Psychology,* 9, pp. 1-14.

Malandrino, D., Petta, A., Scarano, V., Serra, L., Spinelli, R., & Krishnamurthy, B. 2013. Privacy Awareness about Information Leakage: Who knows what about me? In *Proceedings of the 12th ACM Workshop on privacy in the electronic society*, (pp. 279-284). ACM.

Malgieri, G. & Custers, B., 2018. Pricing privacy–the right to know the value of your personal data. *Computer Law & Security Review,* 34(2), pp. 289-303.

Mamonov, S. & Benbunan-Fich, R., 2018. The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior,* 83, pp. 32-44.

Mandal, P., 2018. Qualitative research: Criteria of evaluation. *International Journal of Academic Research and Development,* 3(2), pp. 291-596.

Marwick, A. & Boyd, D., 2011. I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New media & society,* 13(1), pp. 114-133.

Masur, P. K., 2018. *Situational Privacy and Self-Disclosure: Communication Processes in Online Environments.* Cham: Springer.

Mathison, S., ed., 2011. Triangulation. In: *Encyclopedia of Evaluation.* Thousand Oaks: Sage Publications, Inc., p. 424.

Matz, S., Appel, R. & Kosinski, M., 2020. Privacy in the age of psychological targeting. *Current Opinion in Psychology,* 31, pp. 116 - 121.

McChesney, K. & Aldridge, J., 2019. Weaving an interpretivist stance throughout mixed methods research. *International Journal of Research & Method in Education,* 42(3), p. 225–238.

McGavisk, T., 2018. *The Positive and Negative Implications of GDPR.* viewed 24 September 2020, Available at: https://www.timedatasecurity.com/blogs/the-positive-and-negative-implications-of-gdpr

McKim, C., 2017. The Value of Mixed Methods Research: A Mixed Methods Study. *Journal of Mixed Methods Research,* 11(2), pp. 202-222.

McKnight, D., Choudhury, V. & Kacmar, C., 2002. Developing and validating trust measures for e-commerce: An integrative typology. *Information systems research,* 13(3), pp. 334-359.

McLaughlin, C. & Vitak, J., 2012. Norm evolution and violation on Facebook. *New Media & Society,* 14(2), pp. 299-315.

McPeak, A., 2013. The Facebook Digital Footprint: Paving Fair and Consistent Pathways to Civil Discovery of Social Media Data. *Wake Forest Law Review,* 48(4), pp. 887-948.

Mesch, G., 2012. Is online trust and trust in social institutions associated with online disclosure of identifiable information online?. *Computers in Human Behavior,* 28(4), pp. 1471-1477.

Middleton-Leal, M., 2019. *The dangers of oversharing: Why your digital footprint may be putting you at risk online,* viewed 5 September 2020, Available at: https://bdaily.co.uk/articles/2019/11/26/the-dangers-of-oversharing-why-your-digital-footprint-may-be-putting-you-at-risk-online

Millham, M. H. & Atkin, D., 2018. Managing the virtual boundaries: Online social networks, disclosure, and privacy behaviors. *New Media & Society,* 20(1), pp. 50-67.

Min, J. & Kim, B., 2015. How are people enticed to disclose personal information despite privacy concerns in social network sites? The calculus between benefit and cost. *Journal of the Association for Information Science and Technology,* 66(4), pp. 839-857.

Mohamed-Ahmed, A. A-A., 2015. "Sharing is Caring": Online Self-disclosure, Offline Social Support, and Social Network Site Usage in the UAE. *Contemporary Review of the Middle East,* 2(3), pp. 192-219.

Nabity-Grover, T., Cheung, C. M. & Thatcher, J. B., 2020. Inside out and outside in: How the COVID-19 pandemic affects self-disclosure on social media, International Journal of Information Management, viewed 20 August 2020, Available at: https://doi.org/10.1016/j.ijinfomgt.2020.102188

Narayanaswamy, R. & McGrath, L., 2014. A Holistic Study of Privacy in Social Networking Sites. *Academy of Information & Management Sciences Journal,* 17(1), pp. 71-86.

Newk-Fon Hey Tow, W., Dell, P. & Venable, J., 2010. Understanding information disclosure behaviour in Australian Facebook users. *Journal of Information Technology,* 25(2), pp. 126-1236.

Norberg, P., Horne, D. & Horne, D., 2007. The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of consumer affairs,* 41(1), pp. 100-126.

Nouh, M., Almaatouq, A., Alabdulkareem, A., Singh, V., Shmueli, E., Alsaleh, M., & Alfaris, A. 2014. Social information leakage: Effects of awareness and peer pressure on user behavior. In *Proceedings of the 2nd International Conference on Human Aspects of Information Security, Privacy, and Trust*, (pp.352-360). Springer.

Nyoni, P. & Velempini, M., 2015. Data protection laws and privacy on Facebook. *SA Journal of Information Management,* 17(1), pp. 1-10.

Nyoni, P. & Velempini, M., 2018. Privacy and user awareness on Facebook. *South African Journal of Science,* 114(5-6), pp. 27-31.

Öğütçü, G., Testik, Ö. & Chouseinoglou, O., 2016. Analysis of personal information security behavior and awareness. *Computers & Security,* 56, pp. 83-93.

Osman, M., 2019. *Wild and Interesting Facebook Statistics and Facts.* viewed 5 January 2020, Available at: https://kinsta.com/blog/facebook-statistics/

Padyab, A., Päivärinta, T., Ståhlbröst, A. & Bergvall-Kåreborn, B., 2016. Facebook users attitudes towards secondary use of personal information. *In Proceedings of the 37th International Conference on Information Systems*, (pp.1-20). AIS.

Padyab, A., Päivärinta, T., Ståhlbröst, A. & Bergvall-Kåreborn, B., 2019. Awareness of Indirect Information Disclosure on Social Network Sites. *Social Media + Society,* 5(2), pp. 1-14.

Palmieri, C., Prestano, K., Gandley, R., Overton, E & Zhang, Q., 2012. The Facebook Phenomenon: Online Self-Disclosure and Uncertainty Reduction. *China Media Report Overseas, ,* 8(3), pp. 48-53.

Pangrazioand, l. & Selwyn, N., 2018. “It’s Not Like It’s Life or Death or Whatever”: Young People’s Understandings of Social Media Data. *Social Media + Society,* 4(3), pp. 1-9.

Paramarta, V., J. M., Dharma, A., Hapsari, I., Sandhyaduhita, P., & Hidayanto, A. 2018. Impact of User Awareness, Trust, and Privacy Concerns on Sharing Personal Information on Social Media: Facebook, Twitter, and Instagram. In *Proceedings of the 2018 International Conference on Advanced Computer Science and Information Systems*, (pp. 271-276). IEEE.

Peng, G., Nunes, J. & Annansingh, F., 2011. Investigating information systems with mixed methods research. In *Proceedings of the International Workshop on Information Systems Research Trends, Approaches and Methodologies*, (pp. 1-10). IADIS.

Petronio, S., 1991. Communication boundary management: A theoretical model of managing disclosure of private information between marital couples. *Communication Theory,* 1(4), pp. 311-335.

Pham, L., 2018. *A Review of key paradigms: positivism, interpretivism and critical inquiry.* Adelaide: University of Adelaide.

Polisis, 2017. *AI Powered Privacy Policies,* viewed 10 January 2020, Available at: https://pribot.org/

Polisis, 2017. *Polisis.* viewed 10 January 2020, Available at: https://pribot.org/polisis/?_id=5ad9de4cfabac846276d4456&company_url=https%3A%2F%2Fpolicies.google.com&category=first-party-collection-use

Popovac, M. & Hadlington, L., 2019. Exploring the role of egocentrism and fear of missing out on online risk behaviours among adolescents in South Africa. *International Journal of Adolescence and Youth,* pp. 1-16.

Porter, J., 2019. *GDPR Makes It Easier To Get Your Data, But That Doesn’t Mean You’ll Understand It,* viewed 16 January 2020, Available at: https://www.theverge.com/2019/1/27/18195630/gdpr-right-of-access-data-download-facebook-google-amazon-apple

Pötzsch, S., 2009. Privacy awareness: a means to solve the privacy paradox? In: Vashek, M., Fischer-Hübner, S., Cvrcˇek, D., Švenda, P. (Eds.), The Future of Identity in the Information Society. Springer-Verlag, Berlin Heidelberg, pp. 226–236.

Przybylski, A., Murayama, K., DeHaan, C. & Gladwell, V., 2013. Motivational, emotional, and behavioral correlates of fear of missing out. *Computers in Human Behavior,* 29(4), pp. 1841-1848.

Rader, E. 2014. Awareness of behavioral tracking and information privacy concern in facebook and google. In *Proceedings of the 10th Symposium On Usable Privacy and Security*, (pp. 51-67). USENIX.

Rathore, S., Sharma, P.K., Loia, V., Jeong, Y.S. & Park, J.H., 2017. Social network security: Issues, challenges, threats, and solutions. *Information sciences,* 421, pp. 43-69.

Reinecke, L. & Trepte, S., 2014. Authenticity and well-being on social network sites: A two-wave longitudinal study on the effects of online authenticity and the positivity bias in SNS communication. *Computers in Human Behavior,* 30, pp. 95-102.

Rhodes University, 2015. *Rhodes Students Handbook,* Grahamstown: Rhodes University.

Roberts, T. H., 2012. *A Cross-Disciplined Approach to Exploring the Privacy Paradox: Explaining Disclosure Behaviour Using the Theory of Planned Behaviour.* Oxford, AIS .

Robinson, S., 2018. Factors predicting attitude toward disclosing personal data online. *Journal of Organizational Computing and Electronic Commerce,* 28(3), pp. 214-233.

Rosala, M., 2019. *How to Analyze Qualitative Data from UX Research: Thematic Analysis,* viewed 17 January 2020, Available at: https://www.nngroup.com/articles/thematic-analysis/

Rosenberg, E., 2018. *How Google Makes Money.* viewed 11 January 2020, Available at: https://www.investopedia.com/articles/investing/020515/business-google.asp

Rouse, M., 2016. Social Media, viewed 9 September 2020, Available at: https://whatis.techtarget.com/definition/social-media

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

Salt Agency, 2015. *Social Profile Checker,* viewed 6 Decemeber 2020, Available at: https://salt.agency/tools/social-profile-checker/

Saridakis, G., Benson, V., Ezingeard, J. & Tennakoon, H., 2015. Individual information security, user behaviour and cyber victimization: An empirical study of social network users. *Technological Forecasting & Social Change,* 102, pp. 320-330.

Saunders, M., Lewis, P. & Thornhill, A., 2009. *Research Methods for Business Students.* 5th ed. Harlow: Pearson Education.

Saunders, M., Lewis, P. & Thornhill, A., 2016. *Research Methods for Business Students.* 7th ed. Harlow: Pearson Education.

Schermer, B., 2013. Risks of profiling and the limits of data protection law. In: B. Custers, T. Calders, B. Schermer & T. Zarsky, eds. *Discrimination and Privacy in the Information Society.* Berlin: Springer, pp. 137-152.

Schreiber, J., 2012. Descriptive Statistics. In: L. Given, ed. *The SAGE Encyclopedia of Qualitative Research Methods.* Thousand Oaks: SAGE Publications, Inc., pp. 210-212.

Schwaig, K., Segars, A., Grover, V. & Fiedler, K., 2013. A model of consumers' perceptions of the invasion of information privacy. *Information & Management,* 50(1), pp. 1-12.

Serafinelli, E. & Cox, A., 2019. 'Privacy does not interest me'. A comparative analysis of photo sharing on Instagram and Blipfoto. *Visual Studies,* 34(1), pp. 67-78.

Shah, S. & Al-Bargi, A., 2013. Research Paradigms: Researchers' Worldviews, Theoretical Frameworks and Study. *Arab World English Journal,* 4(4), pp. 252-264.

Shane-Simpson, C., Manago, A., Gaggi, N. & Gillespie-Lynch, K., 2018. Why do college students prefer Facebook, Twitter, or Instagram? Site affordances, tensions between privacy and self-expression, and implications for social capital. *Computers in Human Behavior,* 86, pp. 276-288.

Sheldon, P., 2009. I'll poke you. You'll poke me!" Self-disclosure, social attraction, predictability and trust as important predictors of Facebook relationships. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace,* 3(2).

Shillair, R., Cotten, S.R., Tsai, H.Y.S., Alhabash, S., LaRose, R. & Rifon, N.J., 2015. Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behaviour ,* 48, p. 199–207.

Siegrist, M. & Árvai, J., 2020. Risk perception: Reflections on 40 years of research. *Risk Analysis.,* 17(10), p. 1245–1249.

Silic, M. & Back, A., 2016. The dark side of social networking sites: Understanding phishing risks. *Computers in Human Behavior,* 60, pp. 35-43.

Smith, H., Dinev, T. & Xu, H., 2011. Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly,* 35(4), pp. 989-1015.

Spiekermann, S. & Korunovska, J., 2017. Towards a value theory for personal data. *Journal of Information Technology,* 32(1), pp. 62-84.

Spiekermann, S., Korunovska, J. & Bauer, C., 2012. Psychology of ownership and asset defense: Why people value their personal information beyond privacy. In *Proceedings of the 33rd International Conference on Information Systems*, (pp.1-20). AIS.

Statistica, 2019. *Distribution of Instagram users worldwide as of January 2019, by age group,* viewed 24 April 2019, Available at: https://www.statista.com/statistics/325587/instagram-global-age-group/

Stefanone, M. & Jang, C., 2007. Writing for friends and family: The interpersonal nature of blogs. *Journal of Computer-Mediated Communication,* 13(1), pp. 123-140.

Steijn, W., Schouten, A. & Vedder, A., 2016. Why concern regarding privacy differs: The influence of age and (non-)participation on Facebook. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace,* 10(1).

Steinfeld, N., 2016. "I agree to the terms and conditions": (How) do users read privacy policies online? An eye-tracking experiment. *Computers in Human Behavior,* 55, pp. 992-1000.

Stiles, W., 1999. EBMH notebook: evaluating qualitative research. *Evidence-Based Mental Health,* 2, pp. 99-101.

Stutzman, F., Vitak, J., Ellison, N.B., Gray, R. & Lampe, C., 2012. Privacy in interaction: Exploring disclosure and social capital in Facebook. In *Proceeding of the 6th international AAAI Conference on Weblogs and Social Media*, (pp. 330-337). AAAI Press.

Stutzman, F., Capra, R. & Thompson, J., 2011. Factors mediating disclosure in social network sites. *Computers in Human Behavior,* 27(1), pp. 590-598.

Stutzman, F., Gross, R. & Acquisti, A., 2013. Silent listeners: The evolution of privacy and disclosure on facebook. *Journal of Privacy and Confidentiality,* 2(4), pp. 7-41.

Sujon, Z., 2019. Cambridge Analytica, Facebook, and Understanding Social Media Beyond the Screen. In: C. Rowell, ed. *Social Media in Higher Education: Case Studies, Reflections and Analysis.* Cambridge: Open Book Publishers.

Sun, Y., Wang, N., Shen, X. & Zhang, J., 2015. Location information disclosure in location-based social network services: Privacy calculus, benefit structure, and gender differences. *Computers in Human Behavior,* 52, pp. 278-292.

Taddei, S. & Contena, B., 2013. Privacy, trust and control: Which relationships with online self-disclosure?. *Computers in Human Behavior,* 29(3), pp. 821-826.

Taddicken, M., 2014. The 'Privacy Paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Mediated Communication,* 19(2), pp. 248-273.

Tamir, D. & Mitchell, J., 2012. Disclosing information about the self is intrinsically rewarding. *Proceedings of the National Academy of Sciences,* 109(21), pp. 8038--8043.

Taneja, A., Vitrano, J. & Gengo, N., 2014. Rationality-based beliefs affecting individual's attitude and intention to use privacy controls on Facebook: An empirical investigation. *Computers in Human Behavior,* 38, pp. 159-173.

Taraszow, T., Aristodemou, E., Shitta, G., Laouris, Y. & Arsoy, A., 2010. Disclosure of personal and contact information by young people in social networking sites: An analysis using Facebook profiles as an example. *International Journal of Media & Cultural Politics,* 6(1), pp. 81-101.

Tesfay, W.B., Hofmann, P., Nakamura, T., Kiyomoto, S. & Serna, J., 2018. PrivacyGuide: towards an implementation of the EU GDPR on internet privacy policy evaluation. In *Proceedings of the Fourth ACM International Workshop on Security and Privacy Analytics,* (pp. 15-21). AIS.

Thompson, N., McGill, T. J. & Wang, X., 2017. "Security begins at home": Determinants of home computer and mobile device security behavior. *Computers & Security,* 70, p. 376-391.

Tormala, Z., Petty, R. & Briñol, P., 2002. Ease of retrieval effects in persuasion: A self-validation analysis. *Personality and Social Psychology Bulletin,* 28(12), pp. 1700-1712.

Trepte, S. & Dienlin, T., 2014. Risky behaviors: How online experiences influence privacy behaviors. In: B. Stark, O. Quiring & N. Jackob, eds. *From the Gutenberg galaxy to the Google galaxy.* Wiesbaden: UVK, pp. 225-244.

Trepte, S., Teutsch, D., Masur, P.K., Eicher, C., Fischer, M., Hennhöfer, A. & Lind, F., 2015. Do People Know About Privacy and Data Protection Strategies? Towards the "Online Privacy Literacy Scale" (OPLIS). In: Gutwirth S., Leenes R., de Hert P. eds. *Reforming Euro-pean Data Protection Law.* Springer, Dordrecht, pp. 333-365.

Trepte, S., Reinecke, L., Ellison, N.B., Quiring, O., Yao, M.Z. and Ziegele, M., 2017. A cross-cultural perspective on the privacy calculus. *Social Media + Society,* 3(1), pp. 1-13.

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, pp. 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. N*ew Media & Society,* 20(1), pp. 141-161.

Van der Schyff, K. & Flowerday, S., 2019. Social media surveillance: A personality-driven behaviour model. *SA Journal of Information Management,* 21(1), pp. 1-9.

Van Der Velden, M. & El Emam, K., 2013. "Not all my friends need to know": a qualitative study of teenage patients, privacy, and social media. *Journal of the American Medical Informatics Association,* 20(1), pp. 16-24.

Van Lieshout, M., 2014. The Value of Personal Data. In: J. Camenisch, S. Fischer-Hubner & M. Hansen, eds. *Privacy and Identity Management for the Future Internet in the Age of Globalisation.* London: Springer, pp. 26-38.

Van Ooijen, I. & Vrabec, H., 2019. Does the GDPR enhance consumers' control over personal data? An analysis from a behavioural perspective. *Journal of consumer policy,* 42(1), pp. 91-107.

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, pp. 283-297.

Vanclay, F., Baines, J. & Taylor, C., 2013. Principles for ethical research involving humans: ethical professional practice in impact assessment Part I. *Impact Assessment and Project Appraisal,* 31(4), pp. 243-253.

Vannini, P., 2012. Ethics and New Media. In: L. M. Given, ed. *The SAGE Encyclopedia of Qualitative Research Methods.* Thousand Oaks: SAGE Publications, Inc., pp. 278-279.

Varnali, K. & Toker, A., 2015. Self-disclosure on social networking sites. *Social Behavior and Personality: an International Journal,* 43(1), pp. 1-13.

Venkatesh, V., Brown, S. & Bala, H., 2013. Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS Quarterly,* 37(1), pp. 21-54.

Vervier, L., Zeissig, E.-M., Lidynia, C. and Ziefle, M., 2017. Perceptions of Digital Footprints and the Value of Privacy. In *Proceedings of the 2nd International Conference*

on Internet of Things, Big Data and Security, (pp. 80-91). ACM.

Vishwanath, A., 2015. Habitual Facebook use and its impact on getting deceived on social media. *Journal of Computer-Mediated Communication,* 20(1), pp. 83-98.

Vishwanath, A., Xu, W. & Ngoh, Z., 2018. How people protect their privacy on Facebook: A cost-benefit view. *Journal of the Association for Information Science and Technology,* 69(5), pp. 700-709.

Wagner, A., Wessels, N., Bruxmann, 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. 3760 – 3769). AIS.

Wang, T., Duong, T. & Chen, C., 2016. Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International Journal of Information Management,* 36(4), pp. 531-542.

Waterloo, S.F., Baumgartner, S.E., Peter, J. & Valkenburg, P.M., 2018. Norms of online expressions of emotion: Comparing Facebook, Twitter, Instagram, and WhatsApp. *New Media & Society,* 20(5), pp. 1813-1831.

Weinberger, M., Bouhnik, D. & Zhitomirsky-Geffet, M., 2017. Factors Affecting Students' Privacy Paradox and Privacy Protection Behavior. *Open Information Science,* 1(1), pp. 3-20.

Wellington, J. & Szczerbinski, M., 2007. *Research Methods For The Social Sciences.* London: Continuum.

Westin, A., 1967. *Privacy and Freedom.* New York: Atheneum.

Wieringa, R., 2014. *Design Science Methodology for Information Systems and Software Engineering.* Berlin: Springer.

Williams, E. & Yerby, J., 2019. Google and Facebook Data Retention and Location Tracking through Forensic Cloud Analysis. In *Proceedings of the 2019 Southern Association for Information Systems*, (pp. 1-6). AIS.

Wilson, D., & Valacich, J. 2012. Unpacking the Privacy Paradox: Irrational Decision-Making within the Privacy Calculus. In *Proceedings of the 33rd International Conference on Information Systems*, (pp. 4152-4162). AIS.

Winkler, S. & Zeadally, S., 2016. Privacy policy analysis of popular web platforms. *IEEE Technology and Society Magazine,* 35(2), pp. 75-85.

Wirth, J., Maier, C. & Laumer, S., 2018. The Influence of Resignation on the Privacy Calculus in the Context of Social Networking Sites: An Empirical Analysis. In *Proceedings of the 26th European Conference on Information Systems*, (pp.1-16). AIS.

Wirth, J., Maier, C. & Laumer, S., 2019. Subjective norm and the privacy calculus: explaning self-disclosure on social networking sites. In *Proceedings of the 27th European Conference on Information Systems*, (pp.1-17). AIS.

Xu, F., Michael, K. & Chen, X., 2013. Factors affecting privacy disclosure on social network sites: an integrated model. *Electronic Commerce Research,* 13(2), pp. 151-168.

Xu, H. & Tan, B., 2012. Why do I keep checking Facebook: Effects of message characteristics on the formation of social network services addiction. In *Proceedings of the 33rd International Conference on Information Systems,* (pp. 812-823). AIS.

Yao, M., 2011. Self-Protection of Online Privacy: A Behavioral Approach. In: S. Trepte & L. Reinecke, eds. *Privacy Online.* Heidelberg: Springer, pp. 111-125.

Zhao, L., Lu, Y. & Gupta, S., 2012. Disclosure intention of location-related information in location-based social network services. *International Journal of Electronic Commerce,* 16(4), pp. 53-90.

Zhou, T. & Li, H., 2014. Understanding mobile SNS continuance usage in China from the perspectives of social influence and privacy concern. *Computers in Human Behavior,*37, pp. 283-289.

Zillich, A. & Müller, K., 2019. Norms as Regulating Factors of Self-Disclosure in a Collapsed Context: Norm Orientation Among Referent Others on Facebook. *International Journal of Communication,*13, pp. 2632–2651.

Zins, C., 2007. Conceptual approaches for defining data, information, and knowledge. *Journal of the American society for information science and technology,* 58(4), pp. 479-493.

Zlatolas, L., Welzer, T., Heričko, M. & Hölbl, M., 2015. Privacy antecedents for SNS self-disclosure: The case of Facebook. *Computers in Human Behavior,* 45, pp. 158-167.

APPENDIX A: PUBLICATIONS

Parker, H.J. and Flowerday, S.V., 2020. Contributing factors to increased susceptibility to social media phishing attacks. *South African Journal of Information Management*, *22*(1), pp.1-10.

Parker, H.J. and Flowerday, S.V., Understanding the Disclosure of Personal Data Online, *Information and Computer Security*. (Under Review)

APPENDIX B: INSTRUCTIONS FOR DATA RETRIEVAL

Google Data

Step 1 Access your Google Account and login when asked

Step 2 Select **Data and Personalization**

Step 3: Click **Go to ad settings**

Step 4: Click Gmail under **Things to Do**

Step 5: Review Contacts and other Google Services

Step 6: Review **Your Activity Data** (Location, Web and App history and YouTube history)

Instagram Data

Step 1: Go to your profile and click the **gear icon**.

Step 2: Click **Privacy and Security**.

Step 3: Scroll down to **Account Data** and click **View Account Data**.

Step 4: To review a specific type of data, click **View All**

Facebook Data

Step 1: Login to Facebook

Step 2: Click **arrow** in the top right of Facebook, then click **Settings**.

Step 3: In the left column, click **Your Facebook Information**.

Step 4: Next to **Access Your Information**, click **View**.

APPENDIX C: QUESTIONNAIRE AND INTERVIEW SCHEDULE

Questionnaire

The Likert Type Scale for Part A is based on a 4-point scale from Strongly Disagree to Strongly Agree and items based on a 4-point scale from Very Risky to Very Useful in Part B. Control construct questions appear only in questionnaire 1, while question 35 to 37 only appeared in questionnaire 2. All other questions were included in both questionnaire 1 and 2.

Table C. 1 Quantitative Questionnaire

Construct	Number	Question	Reference
Part A			
Control Constructs	1.	What is your gender?	Self-developed
	2.	What is your age?	Self-developed
	3.	How much time per day do you spend on social media?	Self-developed
	4.	How many Instagram followers do you have?	Self-developed
	5.	How many Facebook friends do you have?	Self-developed
Attitude	6.	I am concerned that Facebook and Instagram are collecting too much personal information about me.	Adapted from Lin, X., Featherman, M. & Sarker, S., 2017
	7.	I am concerned that the information I submit on Facebook, Google and Instagram can be used in a way I did not foresee.	Adapted from Krasnova & Veltri, 2010
	8.	It is desirable to protect my personal information on Facebook, Google and Instagram.	Adapted from Chon, et al., 2018
	9.	Disclosing personal information online is a good idea.	Adapted from Chon, et al., 2018

Trust in Social Media provider	10.	Facebook, Google and Instagram are open and receptive to the needs of their members.	Krasnova, et al., 2010
	11.	Facebook and Instagram make good-faith efforts to address most member concerns.	Krasnova et al., 2010
	12.	Online social networks are trustworthy.	Krasnova et al., 2010
Subjective Norms	13.	I feel that most people who are important to me think I should use Facebook, Instagram and Google because these platforms provide many benefits.	Adapted from Min & Kim, 2015
	14.	People who are important to me believe that I should be careful when exposing my information on Facebook, Instagram and Google because my personal information can be at risk.	Adapted from Min and Kim, 2015
Perceived Risk	15.	Overall, I see no real threat to my privacy due to my presence on social networks.	Krasnova et al., 2010
	16.	I fear that something unpleasant can happen to me due to my presence on social networks.	Krasnova et al., 2010
	17.	I am worried that unknown third parties will access my personal information from Facebook, Instagram and Google.	Adapted from Lin, et al., 2017
	18.	Potential risks to the privacy of my information online discourage me from disclosing information.	Self-developed

Perceived Benefits	19.	Using online social networks is convenient to inform all my friends about my ongoing activities.	Krasnova et al., 2010
	20.	I believe sharing information online is positive and has many benefits.	Self-developed
	21.	I get to know new people through Facebook and Instagram.	Krasnova et al., 2010
	22.	I find Facebook, Google and Instagram entertaining.	Adapted from Krasnova et al., 2010
	23.	I am willing to disclose personal information on Facebook, Instagram and Google because of the benefits I get from using these platforms.	Self-developed
FOMO	24.	When I have a good time, it is important for me to share the details online (e.g. updating status).	Przybylski, et al., 2013
	25.	I post regularly on social networks to keep up with my friends.	Self-developed
	26.	It bothers me when I find out my friends are having fun without me.	Przybylski et al., 2013
Personal Valuation of Information	27.	I am aware that my personal information is valuable.	Self-developed
	28.	I feel emotionally connected to my Facebook and Instagram profile and the information I share.	Adapted from Spiekermann & Korunovska, 2017
	29.	I protect my online data because it could potentially be sold to third parties.	Self-developed
Awareness	30.	I am aware that my Facebook and Instagram data can be sold to third parties such as marketing or government agencies.	Adapted from Spiekermann, et al., 2012

	31.	I follow news and the development of problems and violations concerning privacy.	Zlatolas, et al., 2015
	32.	I am aware that social media sites store personal data about me.	Self-developed
	33.	My knowledge of these privacy-related problems makes me believe that my personal information captured on Facebook, Instagram and Google is safe.	Self-developed
Intention to disclose	34.	Overall, I am willing to reveal my personal information such as name, affiliation, job, educational background on Facebook and Instagram.	Adapted from Min and Kim, 2015
	35.	I intend to continue using Facebook rather than discontinue its use.	Adapted from Min and Kim, 2015
	36.	I intend to continue using Instagram rather than discontinue its use.	Adapted from Min and Kim, 2015
	37.	I intend to continue using Google rather than discontinue its use.	Adapted from Min and Kim, 2015
Part B			
Attitude	38.	I think that giving information on Facebook, Google and Instagram that identifies me is:	Adapted from Dienlin and Trepte, 2015
	39.	I think that communicating personal information on Facebook and Instagram is:	Adapted from Dienlin and Trepte, 2015
Subjective Norm	40.	People who are important to me believe communicating personal information on Facebook and Instagram is:	Adapted from Dienlin and Trepte, 2015

Model with Questions from Questionnaires

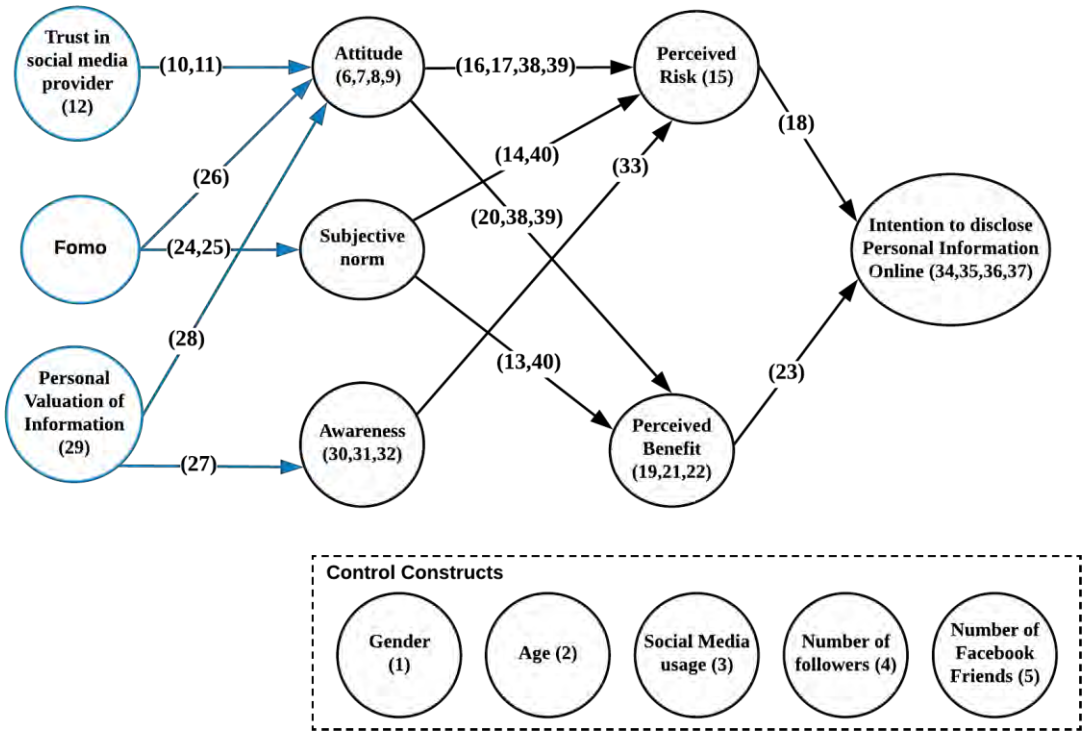


Figure C. 1 Model with Question Numbers

Semi-Structured Interview Schedule After Experiment

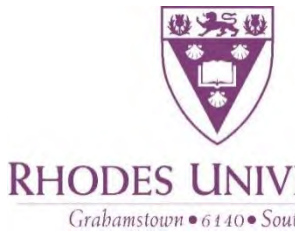
Table C. 2 Qualitative Interview Questions

Construct	Number	Question	Reference
Awareness	1.	How aware were you that Google records your data in this way?	Self-developed
Valuation of Information	2.	How do you feel about your data now that you have been made aware of what is stored?	Self-developed
Attitude	3.	How do you feel about Facebook, Google and Instagram capturing and storing your data?	Self-developed
Attitude	4.	What surprised you about the findings from today?	Self-developed
Attitude	5.	Is online privacy important to you? Please explain your answer.	(Vervier et al., 2017)
Behaviour	6.	How intensively do you protect your data?	(Vervier et al., 2017)
Behaviour	7.	How do you protect your privacy on the Internet?	(Vervier et al., 2017)
Trust	8.	How do you feel about Facebook and Instagram's ability to protect the information you provide?	Adapted from (Krasnova and Veltri, 2010)
Experience	9.	Have you ever had negative experiences online?	Self-developed
Subjective Norms	10.	Do you ever feel that Facebook or Instagram have caused you stress or anxiety?	(Fox & Moreland, 2015)
Subjective Norms	11.	Do you ever feel pressured to use Facebook or Instagram?	Self-developed
Benefits	12.	Do you feel that the benefits of social media encourage you to share more personal information?	(Heravi, et al., 2017)

Risk/ Consequences	13.	Have you ever had physical repercussions from using Facebook, Instagram or Google?	(Fox and Moreland, 2015)
Awareness	14.	After the knowledge you gained today, would you change anything?	Self-developed
Concern	15.	Do you mind if your data is stored offshore?	Self-developed
	16.	Do you have anything you would like to add?	Self-developed

APPENDIX D: PARTICIPANT CORRESPONDENCE

Participant Invitation



INFORMATION SYSTEMS DEPARTMENT

Dear Student

You are being invited to participate in a Masters research project entitled **'An Online Information Security Awareness Model: The Disclosure of Personal Data'.**

The purpose of the intended research is to review the factors that influence a user to disclose personal information online. This study intends to create a model that demonstrates the extent to which awareness, attitudes, and social norms influence a user's perception of the risks and benefits associated with information disclosure online. A small sample of students will complete surveys and be interviewed to determine their awareness surrounding the data stored about them by online platforms.

The invited participants should be active Facebook, Google and Instagram users between the age of 18 and 35.

What participation will entail

Completing two Questionnaires on your information disclosure practices and beliefs, as well as being interviewed by the researcher on the findings from your data request to online platforms and your attitude towards privacy online. Each session should not take longer than an hour.

Voluntary participation and the right to withdraw

As a participant, you have the right to withdraw from participation at any time during the session.

Whom to contact

If you have any questions before you make your decision to participate in the research, or if any questions arise during the course of your participation, please do not hesitate to contact:

Heather Parker
g15p0295@campus.ru.ac.za

The Research Team
Heather Parker is a Masters student at Rhodes University's Department of Information Systems.

Ethics Approval:
This study has received approval from the Rhodes University Ethics Committee.

Concerns
Should you have concerns about the ethics of this research process, please raise them with the principal researcher or alternatively with the researcher's supervisor:

Prof. Stephen Flowerday
s.flowerday@ru.ac.za

Participant Consent Form

RHODES UNIVERSITY
Grahamstown • 6140 • South Africa

INFORMED CONSENT DECLARATION
(Participant)

Project Title: An Online Information Security Awareness Model: The Disclosure of Personal Data

Heather J. Parker from the Department of Information Systems, Rhodes University has requested my permission to participate in the above-mentioned research project.

The nature and the purpose of the research project and of this informed consent declaration have been explained to me in a language that I understand.

I am aware that:

1. The purpose of the research project is to investigate how an increase in awareness of the value of personal information could influence a user to safeguard their personal information.

2. Rhodes University has given ethical clearance to this research project and I have seen/ may request to see the clearance certificate.

3. By participating in this research project, I will be contributing towards increasing my awareness of the data that is stored about me by Facebook, Google and Instagram. Through this awareness and an awareness of ways to protect my data, I will be able to secure my personal information online.

4. I will participate in the project by completing a survey and requesting the data stored about me from Facebook, Google and Instagram. While waiting for my data request to be fulfilled the researcher will show me the data that is publicly available about me on Facebook, Google and Instagram. When the data request has been retrieved, I will be able to see what information these platforms store about me. Following this I will have a discussion with the researcher about these findings and my attitude towards privacy online. Once this discussion is completed, I will complete a final survey.

5. My participation is entirely voluntary and should I at any wish to withdraw from participating further, I may do so without any negative consequences.

6. I will receive a Rhodes University backpack for participating in this study.

7. There are no known risks associated with participation in the project.

8. The researcher intends publishing the research results in the form of a conference paper and a journal article. However, confidentiality and anonymity of records will be maintained and that my name and identity will not be revealed to anyone who has not been involved in the conduct of the research.

9. I will receive feedback in the form of an email regarding the results obtained during the study.

10. Any further questions that I might have concerning the research or my participation will be answered by Heather J. Parker, g15p0295@campus.ru.ac.za.

11. By signing this informed consent declaration, I am not waiving any legal claims, rights or remedies.

12. A copy of this informed consent declaration will be given to me, and the original will be kept on record.

I, …….. have read the above information / confirm that the above information has been explained to me in a language that I understand and I am aware of this document's contents. I have asked all questions that I wished to ask and these have been answered to my satisfaction. I fully understand what is expected of me during the research.

I have not been pressurised in any way and I voluntarily agree to participate in the above-mentioned project.

……. …… …….

Participants signature **Witness** **Date**

Rhodes University, Research Office, Ethics
Ethics Coordinator: ethics-commitee@ru.ac.za
t: +27 (0) 46 603 7727 f: +27 (0) 86 616 7707
Room 220, Main Admin Building, Drostdy Road, Grahamstown, 6139