Gordon Institute of Business Science
University of Pretoria

The impact of the right to be forgotten on privacy and online information disclosure

Nigel Ndaga Mangwanda

458079

A research project submitted to the Gordon Institute of Business Science, University of Pretoria, in partial fulfilment of the requirements for the degree of Master of Business Administration.

9 November 2015

ABSTRACT

The question of how much control individuals have over their data online has taken centre stage with the introduction of the European Union's "right to be forgotten" (RTBF) principle. However, this principle does not explain the impact and possible consequences that this right has on an individual's willingness to disclose information online. This research examines how an individual's privacy calculus is affected if he or she discloses person ally identifiable information online to service providers.

Two hypotheses, the first which, related to the influence the right to be forgotten has on the privacy calculus and, secondly, dealing with the impact of such on information disclosure are assessed using quantitative approach based on an online survey (n=502). The results were analysed using nonparametric tests, which included Spearman's Correlation, Krusal Wallis and the Mann-Whitney U tests.

The findings show that the RTBF principle does influence an individual's thought process prior to he or she disclosing information online. Furthermore, the findings indicated individuals with a medium and high degree of information disclosure would disclose more personally identifiable information if they were convinced that information they provided was not discernible.

Some of the findings in this research could be of significance in the areas of information technology, international and criminal law, psychology, politics and human rights. Additionally, this study could be used to address individual privacy through amendments to privacy policies, laws and changes in software engineering practices.

KEYWORDS

Privacy, Right to be forgotten, Privacy calculus, Privacy paradox, Information disclosure

DECLARATION

I declare that this research project is my own work. It is submitted in partial fulfilment of the requirements for the degree of Master of Business Administration at the Gordon Institute of Business Science, University of Pretoria. It has not been submitted before for any degree or examination in any other University. I further declare that I have obtained the necessary authorisation and consent to carry out this research.

_____

Nigel Ndaga Mangwanda

9 November 2015

ACKNOWLEDGEMENTS

First and foremost, I would like to thank my Lord Jesus for this grace, favour and blessings in my life.

This MBA journey would not have been possible without the support from the following people:

- To my supervisor, Robert Beney, thank you very much for your guidance throughout my research process. I thoroughly enjoyed our discussions on information security, privacy and the road ahead. I will miss our Lorenzino catch-ups.
- To my CEO and sponsor, Michael Prentice, thank you for having faith in me and granting me the privilege of completing my MBA at Africa's leading business school. I am grateful to you and all the Directors at Silica for supporting me on this journey.
- To Pearl Venkatramen, thanks for being my study partner, teacher but most importantly, a friend who always believed in me and kept me motivated throughout this exciting journey.
- To my friend Mari Terblanche for proofreading my research and helping be produce an easily readable research paper and Muhammad Jamal, my statistician, for assisting me in making sense of my survey data and always bringing the magic.
- To Professor Carel van Aardt (from the Bureau of Marketing Research, UNISA) for insightful perspectives on different aspects of the study.
- To my parents Khombe Marcel Mangwanda, Josée Lusungu Mangwanda and Elifa Mavinga, thank you for your love and support throughout the years.
- To my siblings Don, Gloria, Janelle, Mylene and Marcel, thank you all for your encouragement and your understanding when I was not always present.
- To my extended family, Dr Patrick Naidoo, Mrs Vino Naidoo and Sashegan Steve Naidoo, thanks for always being there and giving me words of encouragement.
- To my friend Dido Wa Kalonji, thank you for always keep it real and motivating me. I also extend much appreciation to a friend, mentor and colleague Stuart Micali for keeping me focused on the end goal.
- Lastly, to my wife and best friend, Ronishree, thank you for being my number one supporter. I could not have done this without you by my side. You are my inspiration and I love you very much.

Dedicated to my wife, Ronishree

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

LIST OF ABBREVIATIONS

Abbreviation	Description
AEPD	Agencia Española de Protección de Datos
ANOVA	Analysis of Variance
AVE	Average Variance Explained
CCR	Composite Construct Reliability
CEO	Chief Executive Officer
CJEU	Court of Justice of the European Union
EC	European Commission
EU	European Union
FIP	Fair Information Practices
GPS	Global Positioning System
IBM	International Business Machines
IM	Instant Messaging
KMO	Kaiser-Meyer-Olkin
LBS	Location Based Services
MAR	Missing at Random
MCAR	Missing Completely at Random
MNAR	Missing not at Random
PII	Personally Identifiable Information
RTBF	Right to be forgotten
SNS	Social Networking Site(s)
SPSS	Statistical Package for the Social Sciences
VoIP	Voice over Internet Protocol

1. CHAPTER 1: INTRODUCTION OF RESEARCH PROBLEM

1.1. Introduction

There are very few places in the world where the Internet does not form an integral part of society. It is almost inconceivable to imagine a world without the conveniences afforded by this technology, given its easy accessibility and capacity to facilitate communication and seemingly effortless information transfer (Al-Daraiseh, Al-Joudi, Al-Gahtani, & Al-Qahtani, 2014; Baek, 2014). A multitude of services operate on this platform and provide users with the tools to enable the seamless access, sharing and retrieval of information (Belk, 2014). In addition, the rapid proliferation of the Internet has led to an unprecedented rise in data collection, analysis and distribution (Acquisti, 2010; Kshetri, 2014; Mundie, 2014; Wakefield, 2013). Personal information disclosure has thus become increasingly common in order to obtain the benefits that numerous Internet services offer (Taddei & Contena, 2013). However, once submitted online, it has become nearly impossible to retract this information. Therefore, a problem that has developed in this arena is the ambiguity of control that one has over their personal information once disclosed online.

The seemingly lack of complete control over one's personal information online is a cause of serious concern to users as it poses an immense risk to an individual's privacy. Further propagating this fear is the allure of convenience and free amenities promised by Internet services which often lead to increased self-disclosure by individuals, both voluntarily and involuntarily (Sharma & Crossler, 2014). As a result, there exists a crisis regarding the uncertainty in the level of control an individual has over their information (H. Xu, Dinev, Smith, & Hart, 2008).

Popular Internet services include the use of social media for sharing personal information and search engines which enable rapid searches within the vast repositories of data on the Internet (Acquisti, Brandimarte, & Loewenstein, 2015). Over the last two decades, social networking sites (SNS) have become the fastest developing networking tool as these digital platforms allow individuals to communicate as well as share information about themselves with others in the confines of public or semi-public systems (Boyd & Ellison, 2007; K.-Y. Lin & Lu, 2011). Nevertheless, despite the individual's perceived benefits of convenience that these services offer, individuals are becoming more cautious in adopting these online services (M.-C. Lee, 2009).

The wariness surrounding these services is mainly due to the perceived risks (Culnan & Armstrong, 1999; Keith, Thompson, Hale, Lowry, & Greer, 2013; Morosan & DeFranco, 2015) as well as complexities involving online trust (Bella, Giustolisi, & Riccobene, 2011; Wang & Emurian, 2005). There seems to be good reasons for concerns, especially as concerns regarding privacy have increased in recent years as more firms fall victim to online cyber-attacks.

A perusal of press releases for the 2014 and 2015 year revealed several highly publicised security breaches (Table 1). The increases in cyber-attacks led by both government and teams of individuals who seek to exploit information systems have heightened privacy concerns amongst individuals (Dinev, Hart, & Mullen, 2008; Kim, Wang, & Ullrich, 2012). Despite reassurances by organisations to minimise privacy concerns through the introduction of mechanisms such as privacy policies and vast pro-privacy functionality within online services, privacy breaches remain prevalent and have become highly publicised (Table 1).

Table 1: *Recent cyber-attacks and privacy breaches*

Organisation	Type of breach	Impact
T-Mobile (October 2015)	Breach of confidentiality	Social security numbers, birth dates and other personal information of 15 million subscribers leaked online
American Bankers Association (October 2015)	Breach of confidentiality	Usernames, e-mail addresses and passwords of 6400 subscribers leaked
London's 56 Dean Street clinic (September 2015)	Breach of confidentiality	Names and addresses of 780 patient with HIV mistakenly e-mailed out
WhatsApp (September 2015)	Cyber-attack	Malware vulnerability found on Web version of the software which is accessed by 200 million users
Ashley Madison (August 2015)	Breach of confidentiality	32 million accounts leaked online (names, e-mail and physical addresses, credit card information, sexual preferences)
Thomson (August 2015)	Breach of confidentiality	458 customer information leaked online (e-mail and physical addresses, telephone numbers and flight details)
Web.com (August 2015)	Financial	93 000 customer credit card information compromised
Trump Hotel Collection (July 2015)	Financial	Undisclosed number of credit card information obtained
Alfa Insurance (July 2015)	Breach of confidentiality	86 000 individual's names, addresses, date of birth and social security numbers
Microsoft (June 2015)	Cyber-attack	Microsoft's anti-surveillance site hacked
US Army (June 2015)	Cyber-attack	US Army website hacked and taken offline
LastPass (June 2015)	Breach of confidentiality	Undisclosed amount of accounts breached and passwords leaked online
Woolworths Australia (June 2015)	Financial	Over AU$1.3 million worth of redeemable e-gift cards leaked online

Source: IT Governance Blog, Morgan (2015)

Data has become a valuable commodity (Minkkinen, 2015) and therefore these attacks are of concern to online users as security breaches often result in a vast amount of personal information about individuals being disclosed to the public without their consent. Furthermore, in an effort to offer more personalised content, some companies employ a variety of other inconspicuous data collection tools to solicit additional information about their users (Woo, 2006). Thus, subsequent to a security breach, more information about the individual than was originally explicitly provided by the user becomes publically available (Bergström, 2015).

Due to an increase in the above highlighted incidents, individuals have become more conscience of the level of control they have regarding their personal information

(Acquisti et al., 2015; Caudill & Murphy, 2000; Culnan & Armstrong, 1999; Wu, Huang, Yen, & Popova, 2012). This has compelled organisations to identify factors that influence online information disclosure to minimise these risk perceptions. Despite literature providing much insight on a variety of topics relating to information privacy, including matters relating to online trust (Friedman, Khan Jr, & Howe, 2000; Lai, Tong, & Lai, 2011), reasons for concern (Bergström, 2015; Mohamed & Ahmad, 2012) and the need for control (Aaron Gabisch & R. Milne, 2014; Taddei & Contena, 2013), there is limited information regarding the recent concept of the "right to be forgotten" (RTBF) and its impact on privacy and individual information disclosure.

Entrenched in the European Union's (EU) Data Protection Regulation, the core of the RTBF principle is to empower individuals by giving them the ability to have certain online information about them erased so as to not be indefinitely linked to their past (Ambrose & Ausloos, 2013; Bunn, 2015). In an era where most actions performed online are recorded, syndicated and undeletable, the RTBF principle aims to minimise privacy concerns. This can be achieved by providing individuals with more control over their personal information, within certain parameters that balance individual and societal views on matters. Though highly topical, the notion of requesting to be "forgotten" has received mixed reactions from academics, policymakers and businesses (Brady, 2014; King, 2014; Larson, 2013; Zittrain, 2014). However, this principle is yet to be empirically tested as a variable that can influence an individual's information disclosure patterns.

The study therefore aims to bridge the gap in literature regarding the impact that the RTBF principle has on privacy and individual information disclosure. In so doing, the result of this research may allow companies to find new and innovative ways of reassuring individuals that their online privacy remains a priority.

1.2. Background

The Internet never forgets (Almeida, 2012). The exponential growth of the digital age has resulted in companies requesting more information from individuals, often without a clear specification of how the information collected will be used. For organisations, information disclosed by individuals through online services provides comprehensive datasets that can be used for, among other things, business analytics, improved marketing and employee screening (Aaron Gabisch & R. Milne, 2014; Chiang & Suen, 2015). Inherent to such disclosures are the theme of risk versus benefits (trade-offs) and the dynamics of trust in social contracts between individuals and organisations.

Thus, prior to the disclosure of personal information when online, individuals perform a mental calculation (called the privacy calculus) which assesses the anticipated risks and benefits associated with such an action (Culnan, 1993).

Despite the privacy calculus, the actions of individuals towards online information disclosure are often not always aligned to their persistent expression of privacy concerns (Norberg, Horne, & Horne, 2007). The term privacy paradox has become synonymous with the uncertain, if not paradoxical nature of individuals privacy intention and their actual behaviour. The paradox continues to be debated extensively in literature by information privacy scholars in an effort to improve its effect on human behaviour within an online context (Baek, 2014; Dienlin & Trepte, 2015).

Debates regarding how privacy should be regulated online have generated thought-provoking views between government-led regulations and self-regulation (Corbett, 2013; Culnan, 2000). It is against this backdrop that the notion referred to as the "right to be forgotten" was introduced in January 2012 by the Court of Justice of the European Union (CJEU). The RTBF principle empowers EU citizens with a legal apparatus of control regarding how their personal information is processed and disseminated beyond the point of disclosure (Ausloos, 2012).

Under the RTBF principle, organisations have a legal obligation to comply with information erasure requests from individuals who deem that certain information pertaining to them as inaccurate, irrelevant or excessive (European Commission, 2014). Logically, the interference by government on social issues driven within the free-market context of the Internet has been met with much contention amongst academics (Mantelero, 2013; Rees & Heywood, 2014) and organisations (Brady, 2014; King, 2014; Zittrain, 2014). Much of the critique stems from the fact that policies such as the RTBF principle can affect the preservation of history, introduce censorship and limit the freedom of expression (Larson, 2013).

The privacy calculus undertaken by individuals has been sufficiently debated (Keith et al., 2013; Knijnenburg, Kobsa, & Jin, 2013; Min & Kim, 2015), however no empirical research could be found that factored in the implications of legal frameworks on this calculus. This is with the exception to Rolf H. Weber (2010) and Westin (2003) who allude to challenges with such approaches, though not specifically directed towards the RTBF. Additionally, no academic research has been found thus far that informs organisations on how the integration of the RTBF principle influences behavioural drivers of online information disclosure amongst individuals.

The study at hand thus seeks to contribute to existing literature on the privacy calculus, by investigating whether the RTBF principle has any influence on an individual's decision-making process when disclosing information online. In so doing, the data generated by this study may assist organisations in better understanding individual online behaviours when provided with varying degrees of control over their data, including its erasure. The results also have the potential to be interdisciplinary in nature due to its applicability across many fields, including but not limited to – information technology, international and criminal law, psychology, politics and human rights.

1.3. Research Problem

Based on the background above, the primary research objective of this study is to establish whether the RTBF influences the privacy calculus of individuals when disclosing information online. A secondary objective flowing from the primary objective is to assess whether the RTBF has an impact on information disclosure amongst individuals. From an academic perspective, given the topical nature of the RTBF and its prominence in the press (Gibbs, 2015; Jenkins, 2015; Manjoo, 2015; Peters, 2015), there is a need for new insight into this phenomenon and its impact on existing theories regarding information privacy.

1.4. Scope and Limitations of the Research

The research primarily focuses only on aspects related to the erasure of personal information that individuals provide to online service providers be it knowingly or unknowingly. The RTBF principle, in its entirety, is reviewed in more detail in Chapter 2. Online service providers are limited to organisations that provide a platform that facilitates interactions between individuals while online in the context of this study. SNS are one of the platforms that encourage the most amount of personal information disclosure and therefore the main focus of this research will be on this area (Taddei & Contena, 2013).

Given that the RTBF principle originates from the European Union judiciary system, in order to recognise how this propagating principle would be perceived among various nationals of the sample population (described in Chapter 4), this research ignores the constraints of geographical restrictions that are imposed by the CJEU. The reason for this is to understand whether the applicability of the RTBF is in any way beneficial to those outside the confines of the EU. To this extent, two hypotheses regarding the RTBF are outlined in Chapter 3. It is further noted that although there exists methods to

aid in the implementation of systematic erasure of online data (Mayer-Schönberger, 2011), this research does not cover the technical implementation of the principle.

1.5. Structure of Research Paper

The remainder of this research paper is organised into six chapters. Chapter 1 provided insights and details of the study. A literature review of some of the more pertinent aspects of RTBF principle are considered in Chapter 2. Chapter 3 outlines the research hypotheses and provides a conceptual model of the research. Chapter 4 provides insight into the research methodology selected. The results of statistical tests ran against the research instrument are provided in Chapter 5, followed by a discussion of these results in Chapter 6. Lastly, implications of the research are provided, limitations outlined and directions for future research are suggested in Chapter 7.

1.6. Conclusion

Chapter 1 has outlined reasons related to privacy concerns that affect individuals when utilizing online services. Examples regarding the high uptake of SNS usage and the impact of privacy breaches were highlighted to emphasise the magnitude and severity that organisational security failures can have on individuals.

Related to the topic of information privacy, a brief introduction into the principle known as the “right to be forgotten” was provided. The subsequent chapter will review the pertinent and current literature regarding information privacy. Particular emphasis will be placed on constructs pertaining to factors influencing an individual’s privacy calculus and the RTBF principle.

2. CHAPTER 2: LITERATURE REVIEW

2.1. Introduction

The current digital era, with all its advantages and ease of accessibility, introduces an element of concern to users regarding the disclosure of their personal information. Users engage in a privacy calculus conundrum, weighing the risks and benefits with each intention to disclose information online. In Chapter 1, the concern of users regarding the lack of complete control over their personal information was established. Current breaches and violations were highlighted and used to corroborate the concern surrounding information disclosure.

Chapter 2 covers the relevant literature pertaining to information privacy through a critical assessment of recent literature in the fields of information technology, human behaviour, consumer marketing and law. The chapter begins with insight into what constitutes online information disclosure, variants of privacy as well as understanding factors affecting the privacy calculus. Furthermore, a look at the social contracts between individuals and the organisations within an online context by assessing how breaches in these contracts lead to privacy concern. Once the foundation of these concerns are understood, the RTBF as a mechanism that provides individuals with more control over their personal information is assessed and its applicability discussed.

2.2. Online Information Disclosure

2.2.1. Privacy

The Internet is an information highway accessed by over 2.8 billion people (Euromonitor International, 2015). In this digital era, information has become easily accessible to any person that has a connection to the Internet. However, once this information is made available online, it can rarely be removed, thereby leaving one's footprints scattered across the Internet (Bergström, 2015). This begs the question "What is privacy?"

The seminal works of privacy by Westin (1968, p. 7), define 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. Viewed in terms of the relation of the individual to social participation, privacy is the voluntary and temporary withdrawal

> of a person from the general society through physical or psychological means, either in a state of solitude or small group intimacy or, when among large groups, in a condition of anonymity or reserve."

Despite many dimensions of privacy, e.g. emotional and physical, this research focuses specifically on information privacy. Taddei and Contena (2013, p. 822) define information privacy as "a process of anonymity preservation which is strongly connected with control over information about the self", a definition in line with Westin (1968).

Personal information has been classified in literature by Sharma and Crossler (2014) as items which include "physical addresses, e-mails, pictures, social security numbers, and credit card numbers" and therefore differs between individuals. Related to personal information is the concept of personally identifiable information (PII), which is any data that can be used to distinguish individuals from one another (Narayanan & Shmatikov, 2010; Schwartz & Solove, 2011). Whilst a relatively straightforward concept in theory, the application of PII in the current digital age can be complex. The reason for this is due to the fluid nature of PII, i.e. what is regarded as identifiable and non-identifiable information (Schwartz & Solove, 2011)?

The ambiguity of PII appears evident when individuals engage in online transactions. Studies have shown that individuals are more willing to reveal PII on SNS platforms such as Facebook when the receiving party shares the equivalent amount of information (Venkatanathan, Kostakos, Karapanos, & Gonçalves, 2013), which is in contradiction to their heightened sense of privacy concern (Barnes, 2006). This pattern of behaviour obscures the lines of privacy as it increases and individual's exposure to exploitation if the receiving party has malicious intent regarding the disclosed information (Venkatanathan et al., 2013).

In addition to SNS, the evolution of the Internet has brought about a plethora of ways in which one can share information, including using traditional computing (laptops and desktop machines) and more recently, "smart devices" (Poslad, 2011). In the case of smart devices, the introduction of devices with built-in sensors able to detect an individual's pulse, distance travelled and even recognise their fingerprints has introduced new dimensions to how information is collected and subsequently shared. Examples include the use of Fitbits© to track cardiovascular measures, SmartTVs which adapt content based on watching habits and smartphones that use location based services (LBS) to recommend information based on an individual's current

position. With each example comes a level of information disclosure required by the user (the individual using the service) to ascertain a more personalised experience. H. Xu, Luo, Carroll, and Rosson (2011) found that with the correct mechanisms to control what is construed as private data by means of adjustable privacy settings, individual privacy concerns can be pacified.

With so many innovative ways of gathering data, the line between what constitutes private and public information has become blurred. Questions that arise from such observations include – Should a repository of one's pulse rate be regarded as private information? Is information considered private when economic gain is obtained through its voluntary disclosure? (Tucker, 2012), Should technologies such as "cookies" embedded in Internet browsers be regarded as private? How so if said technologies offer greater personalization that result in improved services to the individual (Awad & Krishnan, 2006; Sutanto, Palme, Tan, & Phang, 2013)?

These questions implore for a new definition of what constitutes personal information in today's digital era. Integral to the concept of privacy, an understanding of the antecedent of information disclosure is needed prior to deliberating factors that influence an individual's privacy calculus.

2.2.2. Disclosure

Literature has provided comprehensive insight into personal information disclosure when online, specifically on SNS (Sharma & Crossler, 2014; F. Xu, Michael, & Chen, 2013). Studies have highlighted that individuals disclose information for a multitude of reasons including social interaction, personalisation and financial reward (Smith, Dinev, & Xu, 2011; Sutanto et al., 2013). Given the substantial growth rate in content, the Internet has become the largest repository of data containing content provided by users in multiple forms, including – through the use of blogs, collaborative sharing, peer to peer sharing and social networks (Botsman & Rogers, 2011; Boyd & Ellison, 2007; Jackling, Natoli, Siddique, & Sciulli, 2014). These examples can be encompassed as passive or voluntary disclosure in that consent by the individual is provided for the disclosure of such information to others, as is the case with SNS (Trepte & Reinecke, 2013).

Information disclosure can also occur involuntarily and this arises when the user is unaware that they may be disclosing more information than is intended. A suitable example of involuntary disclosure is the geo-location information found in image metadata (property fields such as size, camera type used, etc.). Despite the intention to

share a heartfelt moment with family, friends or colleagues, users inadvertently disclose information about their whereabouts – in this case, their exact GPS location of where the photo was taken. Such disclosure of an individual's personal information can be of concern when it infringes on their privacy. Acquisti et al. (2015) proposed that an individual's concern about privacy is aroused when there is an uncertainty about how their data is being used.

Although there appears to be an elevated level of concern amongst individuals regarding privacy and the disclosure of their personal information, the behaviour displayed by individuals when performing actions online do not always correlate with their concern (Norberg et al., 2007), a phenomenon referred to in literature as the privacy paradox. In particular, users of SNS indicate concern about their online privacy, but very few individuals have the appropriate privacy settings on their online profiles (Gross & Acquisti, 2005). It has also been shown that in terms of PII, users of SNS have higher risk-taking tendencies towards information disclosure than those who do not (Fogel & Nehmad, 2009).

The disclosure of PII on SNS illustrate evidence of a trust relationship between individuals and the organisation managing the SNS platform. This trust level appears to yield some form of understanding between the parties regarding how disclosed information should be treated in a manner that does not prejudice either party, leading to an agreed social contract (H. Li, Sarathy, & Xu, 2011).

2.2.3. Social Contract Theory

Social contract theory postulates that individuals enter into relationships with organisations when information exchange occurs. The relationship can be explicit (legal) or implicit (social) in nature and are governed by certain principles which include (Donaldson & Dunfee, 1994):

- Defined ethical norms agreed on between the parties and
- Informed consent by the parties with the ability to exit.

Relating to information privacy, social contracts are defined as "the commonly understood obligations or social norms for the parties involved" (Yuan Li, 2012, p. 474). When using online services, individuals enter into sustainable relationships with service providers. These relationships are mutually beneficial to users and organisations, with users being allowed to utilise the service whilst the organisation is provided with adequate data (Bergström, 2015). In assessing an organisation's compliance to the

principles of social contract theory, it can be inferred that ethical norms are agreed upon through the acceptance of privacy policies that have proved effective if clearly worded and reduced in complexity (Capistrano & Chen, 2015). With the changing perceptions of what users consider as private information, coupled with increased data collection exercises by organisations, there may exist areas of such practices that could be misconstrued as dishonourable. Examples include the sharing of an individual's personal information with third parties without explicit permission from the individual thus constituting a breach in the social contract.

A point of contention regarding the social contract theory is the lack of clarity regarding the ownership and control of the disclosed data by individuals with another party. According to De Wolf, Willaert, and Pierson (2014), individuals become co-owners with others when they disclose personal information online, thus postulating that others have the same right as the disclosing individual to view and share such information. This perception of ownership contradicts Martin (2015, p. 11) who states that "privacy as a social contract allows for the fact that individuals disclose information without relinquishing privacy", therefore suggesting that individuals consider information shared as an exclusive exchange to only those entitled to see such information (Young & Quan-Haase, 2013).

Whether knowingly or unknowingly, information sharing is occurring at a staggering rate (Hew, 2011) and users are becoming increasingly more concerned with the level of access others have to their personal information (Young & Quan-Haase, 2013). Naturally, individuals have become more hesitant prior to information disclosure and continuously deliberate the associated risks and benefits in doing so.

2.3. Privacy Calculus

Enquiries into how individuals weigh perceived risks to benefits when disclosing information has given rise to the privacy calculus theory (Culnan & Armstrong, 1999; Dinev & Hart, 2006). Privacy calculus posits that individuals engage in a decision-making process (the calculus) prior to disclosing information for a transaction. The theory has been applied to various scenarios including how individuals disclose information for online transactions and disclosure patterns when there are economic benefits. As illustrated in Figure 1, when an individual engages in the privacy calculus, they weigh out the factors pertaining to risks and benefits. When the level of risk increases, the perceived benefits decrease and vice versa.

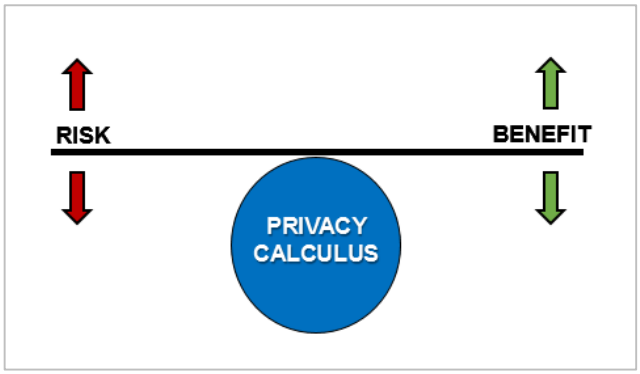

Figure 1: *A representation of the privacy calculus encountered by individuals. A model illustrating the weighing of options when engaging in the privacy calculus to decide on information disclosure. Source: Researcher's own construction.*

In an online environment, individuals are often subject to the opinion of others. This is owing to the fact that although a person may classify certain information as private, there is no guarantee that a broader audience may view the information in the same manner (Martin, 2015). Furthermore, in the event of a breach in confidentiality, the individual who originally disclosed the information may not be aware that such an incident has occurred (Afroz, Islam, Santell, Chapin, & Greenstadt, 2013). The reason for this illusion is the multitude of mediums that can be utilised for such disclosures, for example: e-mail, Voice over Internet Protocol (VoIP), Instant Messaging (IM) or chat rooms.

A study by Mesch (2012) has shown that despite the virtual divide between the Internet and the physical world, individuals have demonstrated similar disclosure patterns within the two environments. Although users may use different personas as a camouflage when on the Internet, the findings indicate that disclosure transcends activities performed online. After canvassing the literature, the most prominent factors that influence the privacy calculus are discussed below and summarised in Table 2.

2.3.1. Factors that Discourage Individual Information Disclosure

The currency of the Internet is information (Bergström, 2015). However, the decision to share one's personal information can be quite challenging as it is compounded by numerous factors.

2.3.1.1. The Lack of Awareness (Need for Awareness)

The Oxford Online Dictionary (2015) defines awareness as "knowledge or perception of a situation or fact" and is a concept that influences an individual's decision to disclose

personal information. In a privacy context, awareness can take the form of knowing how the information that one discloses is being used as well as where the information is being distributed (Pötzsch, 2009). If an individual is cognisant of the risk involved in sharing information, they can be empowered to make an alternative decision that may reduce the likeliness of a breach of their privacy, although behavioural economics have shown that this is often not the case (Shleifer, 2012).

SNS have become platforms which encourage the most amount of information sharing owing to the continuous amount of disclosure which occurs as a means of keeping friends and connections updated on life events (Nicole B Ellison, Charles Steinfield, & Cliff Lampe, 2007). Information disclosed to a specific audience may in turn be further distributed without the disclosing entity's consent, introducing increased risk to their privacy (Hélou, Guandouz, & Aïmeur, 2012). It has also been shown that in recent years that there has been an increase in an individuals need for privacy awareness especially with regard to SNS (Acquisti & Gross, 2006; Mvungi & Iwaihara, 2015). To assist individuals in being more alert regarding the audience they elect to disclose information to, SNS providers have developed various tools to aid individuals in selecting the appropriate privacy settings (Cetto et al., 2014; Hélou et al., 2012; Kang & Kagal, 2010; Malandrino et al., 2013). The construction of these tools stem from the need for individuals to be more aware of who their information is disclosed to, thus, the absence of being aware of this can discourage information disclosure and potentially increase the risk of privacy infringement.

2.3.1.2. Lack of Perceived Control

An individual's awareness of their personal information distils from the ability to have control over the information they choose to share. Perceived control is central to privacy as it provides individuals with the surety that their personal information be used in the intended manner. Hajli and Lin (2014) define perceived control on SNS as ''the extent to which an individual feels that SNS allows that individual to control the use of information through privacy settings''. An increase in the level of perceived control has been correlated with an increase in information disclosure (Stutzman, Capra, & Thompson, 2011). Therefore, it can be inferred that the lack of perceived control may be a point of contention and cause of concern that may reduce information disclosure.

In the case of SNS, the influence of perceived control has been demonstrated to be an important factor regarding an individual's information-sharing patterns (Hajli & Lin, 2014). Brandimarte, Acquisti, and Loewenstein (2012) debated that providing a higher

level of control to individuals actually increases their inclination to divulge more information making them more vulnerable, therefore creating what the authors term, a "control-paradox". Thus, whilst an increase in perceived control may provide an individual more comfort in sharing information online, the lack of control often leads to increased anxiety regarding their privacy (Young & Quan-Haase, 2013).

2.3.1.3. Privacy Concern

The nature of what can be considered as private is an evolving concept. Privacy concerns have been discussed in a multitude of disciplines such as journalism, economics and information science. Broadly defined, privacy concerns express an individual's discomfort regarding their personal information. Preibusch (2013), Wu et al. (2012), Culnan (1993) and Cohen and Hiller (2002) argue that consumer apprehension and privacy concern arise due to the loss of control during the collection, access and utilisation of the individual's personal data. Further studies by Min and Kim (2014) have also corroborated this.

The impact of privacy concern on information disclosure remains elusive due to the privacy paradox concept. Studies have provided evidence that privacy concerns have an impact on information disclosure (Eastlick, Lotz, & Warrington, 2006; Lo, 2010; Utz & Krämer, 2009; Väänänen-Vainio-Mattila, Wäljas, Ojala, & Segerståhl, 2010) however, scholars within the field of privacy conversely contend that no direct relationship exists between privacy concern and information disclosure (Acquisti & Gross, 2006; Debatin, Lovejoy, Horn, & Hughes, 2009; Taddicken, 2014; Tan, Qin, Kim, & Hsu, 2012; Tufekci, 2007).

In summary, privacy concerns can be perceived as a risk to an individual in situations whereby there is ambiguity in the usage of their personal information owing to their loss of control of such information (Acquisti et al., 2015).

2.3.2. Factors that Promote Individual Information Disclosure

Despite the element of risk associated with information disclosure, research that study the perceived benefits individuals obtain when disclosing information online remains an interesting and growing subject matter within social science.

2.3.2.1. Trust

A variable of the privacy calculus theory is trust. Trust is defined as the "belief that someone or something is reliable, good, honest, and effective" (Merriam-Webster,

2015). However, the complexities inherent to the Internet have highlighted that individuals are more likely to trust other people than the technologies utilised (Friedman et al., 2000).

Trust, a factor that may partially explain the "privacy paradox", was alluded to in the preceding sections. If users have trust in the SNS as well as in members of the site, then they would be more willing to disclose information (Acquisti & Gross, 2006; Krasnova, Spiekermann, Koroleva, & Hildebrand, 2010). An individual's trust in the service provider is based on the premise of integrity and honesty that the information disclosed will be used as intended (McKnight, Choudhury, & Kacmar, 2002). However, the interaction between trust and information disclosure can occur either indirectly or directly. It has been argued by Zimmer, Arsal, Al-Marzouq, and Grover (2010) that trust is merely a condition required by an individual before disclosing information thus having an indirect effect. On the other hand, Fogel and Nehmad (2009), Frye and Dornisch (2010) and Mesch (2012) argue that because trust acts as a factor that reduces risk, it would directly affect information disclosure (C. M. K. Cheung & Lee, 2006; Gefen, Rao, & Tractinsky, 2003; Zimmer et al., 2010).

There also exists a relationship between trust and perceived control. If an individual has a higher level of perceived control, it provides a sense of comfort regarding the management of their information, thereby increasing their level of trust and as a result, increasing information disclosure (Joinson, Reips, Buchanan, & Schofield, 2010; Taddei & Contena, 2013). Therefore, trust is a factor that can assist to mitigating perceived risks associated with information disclosure.

2.3.2.2. Perceived Benefits

Perceived benefits, in the case of SNS, is an umbrella term that encompasses various factors including the convenience of maintaining relationships, enjoyment and personalisation (C. M. K. Cheung, Chiu, & Lee, 2011; Krasnova et al., 2010; F. Xu et al., 2013). In the current fast-paced world, mechanisms such as SNS that favour easy communication streams are highly favoured. SNS facilitate the maintenance of relationships by providing a platform that is easy to use, convenient and time efficient (Ahn, Han, Kwak, Moon, & Jeong, 2007; Chen & Marcus, 2012; Hew, 2011; Hui, Tan, & Goh, 2006). These are important determinants that incite users to disclose more information (C. Cheung, Lee, & Chan, 2015; Krasnova et al., 2010).

The same factors required for maintaining relationships are necessary for building new relationships and social capital. Social capital is achieved when individuals interact with

communities with whom they share similar interests and obtain resources through these established relationships (Nicole B. Ellison, Charles Steinfield, & Cliff Lampe, 2007; F. Xu et al., 2013). SNS provide an ideal platform for an individual to gain social capital. A common necessity for building new relationships and establishing social capital is the willingness of participating individuals to disclose personal information (Nicole B. Ellison et al., 2007). Therefore, an individual would be prompted to disclose information should they wish to obtain these goals. Personalisation can be defined as "the ability to provide content and services that are tailored to individuals based on knowledge about their preferences and behaviours" (Adomavicius & Tuzhilin, 2005, p. 83). The need to have services tailored to one's specific requirements can therefore be a motivating factor to disclose personal information that even prevails over an individual's privacy concerns (H. Xu et al., 2011). Another influential factor for information disclosure is the enjoyment aspect that SNS provide (Krasnova et al., 2010; K.-Y. Lin & Lu, 2011). This has been substantiated by Hui et al. (2006) who illustrated that positive experiences encourage users to disclose more information.

2.3.3. Risks vs. Benefits

Inherent in all the above examples and various other similar offerings is that an exchange of personal information has become the de facto requirement to enjoy the benefits of many Internet services (Bergström, 2015). Additionally, individuals are often required to accept privacy policies which act as a form of social contract between the service provider and user (Adkinson, Eisenach, & Lenard, 2002). Many mechanisms have been developed by organisations to alleviate privacy concerns of individuals as previously alluded. Privacy policies have proved to increase confidence in a website when clearly visible and comprehensible (Wu et al., 2012). For a large majority, a motivator to read policies is rooted in wanting to know the extent of control they possess over their personal information (Milne & Culnan, 2004).

However, when choosing to disclose information, an individual engages in the privacy calculus and weighs out the various risks and benefits. In situations where the perceived risks outweigh the benefits, an individual may be discouraged to disclose information (Figure 2A). Numerous studies (C. Cheung et al., 2015; Krasnova et al., 2010; Sun, Wang, Shen, & Zhang, 2015; F. Xu et al., 2013) have indicated that often the perceived benefits can surmount the risks and thus persuade an individual to disclose more personal information (Figure 2B).

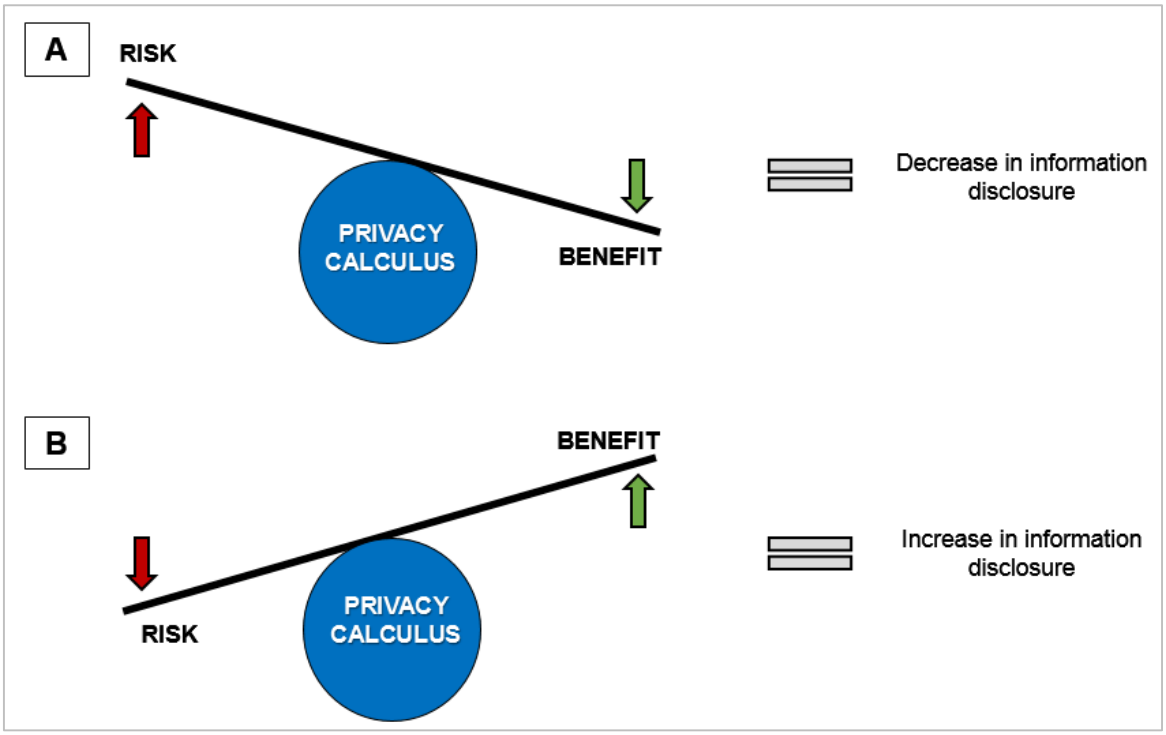

Figure 2: *The effect of factors involved in the privacy calculus. Information disclosure decreases when risks are high, but increases when the benefits outweigh the risks. Source: Researcher's own construction.*

Nonetheless, with information sharing growing and the borders of privacy becoming more blurred, individuals will continue to engage in the privacy calculus and therefore new factors that influence this decision need to be investigated.

Table 2: *Privacy calculus: Summary of construct definition*

Construction	Definition	Literature (adapted from)
Privacy Concern	"An individual's expectation that a high potential for loss is associated with disclosing personal information on social networking sites"	Malhotra, Kim, and Agarwal (2004)
Need for Awareness	"The attention, perception and cognition of whether others receive or have received personal information about him/her" (paraphrased)	Pötzsch (2009)
Perceived Lack of Control	"Representation of the control of transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or minimise vulnerability" (the converse of this statement) or "The extent to which an individual feels that SNS allows that individual to control the use of information through privacy settings" (the converse of this statement)	Doherty and Lang (2014)
Perceived Benefits	"Direct and indirect advantages which an individual obtains. Direct advantages refer to immediate and tangible benefits that customers would enjoy by using a product or service and Indirect advantages are those benefits that are less tangible and difficult to measure." (rephrased)	M. Lee (2008)
Trust	"An individual's beliefs reflecting confidence that personal information submitted to the SNS will be handled competently, benevolently, and with integrity by the SNS"	Mayer, Davis, and Schoorman (1995) and McKnight et al. (2002)

2.4. Information Infringements

2.4.1. Privacy Breaches

Information privacy breaches can be extended from inconspicuous monitoring to various other intrusive artefacts such as spam, unsolicited calls, popup banners, and malware (Wu et al., 2012). As technology evolves, this list will continue to grow and in the future may include unsolicited spying through the use of unmanned aircraft systems, e.g. drones (Finn & Wright, 2012). Technologies such as drones will begin to infringe on other dimensions of privacy, namely physical privacy. The predicted expansion of information privacy breaches thus highlights the core importance of understanding of the concept of information infringement. Within a macro-level, Whitman (2004, p. 1154) aptly alludes that privacy is a "slippery concept" due to differing views of what is considered private from one society to another. Current affairs have illustrated that cyber warfare and security breaches are on the rise (Dinev et al., 2008). Leaks about government spy efforts such as the Snowden revelations have exposed just how deeply rooted government surveillance has become (Johnson et al., 2014; von Solms & van Heerden, 2015). The revelation of top-secret data collection programs like PRISM has further heightened privacy concern. According to a 2014 national poll, 80% of Americans surveyed expressed strong concern towards government monitoring of electronic communications and phone calls (Madden, 2014).

The growing concern of privacy breaches have made individuals more risk-averse and more reluctant to disclose personal information online. Notwithstanding the above, individuals continue to share often intimate information on SNS (Ku, Chen, & Zhang, 2013). Not only does this confirm existing literature on the privacy paradox, but also implies that individual consideration of private information may not be as universally defined.

Personal information theft is now cited as the biggest privacy concern on SNS as it facilitates the misuse of personal information for malicious intent through the extraction of PII (Al-Daraiseh et al., 2014). Intricate details about individuals have become high commodities in cybercrimes. These crimes range from credit card theft to corporate espionage. The increased ability for computers to process terabytes of data has seen the birth of big data. This new data processing method of cross correlating random data can provide better analytical insight (Cumbley & Church, 2013) or infringe on information privacy if used maliciously. With no mechanism to gain full control of their

personal information online, principles that can provide the user more control are becoming imperative to minimise privacy violations.

Indeed privacy violations have occurred because of technologies such as big data. Wu et al. (2012, p. 606) categorise violations as follows:

- Collection of personal information without notification
- Profit by selling personal information
- Personal information redevelopment

Therefore, privacy violations form an integral basis for this research. Investigating what individuals consider as private may facilitate easier categorisation of such information by organisations. Additionally, organisations could superimpose disclosure patterns observed to understand how a customer would react to such information requests. Inherently, by instilling a sense of comfort for information disclosure, organisations are likely to lower current individual privacy concerns (Hinduja, 2004). It is therefore necessary to assess the factors that are taken into consideration when an individual discloses information online. Related to this, it is crucial to understand the different strategies employed by users to safeguard themselves when using online services (De Wolf et al., 2014; Young & Quan-Haase, 2013).

2.4.2. Breaches by Organisations

According to Bansal and Zahedi (2015), organisations have been known to be complicit to privacy violations. The repercussions of such violations include the loss of customers and as a result, a reduction in revenue is observed. Restoration of institutional trust may come at considerable cost to the organisation or, in some cases, it may never occur (Bansal & Zahedi, 2015).

Although certain principles prohibit third party disclosure, companies often hold user data for periods of time that usually extends past their usage cycle. Preserving such information comes with added risk to individuals. Online hackers may expose data pertaining to the individual once they have breached the information security defences put in place by the organisation. Culnan and Armstrong (1999) however argue that organisations that make use of fair information practices (FIP) reduce perceived risk perceptions when these data collection practices are disclosed to individuals, a view supported by Wolf (2014). The disclosure of what data a website collects has gained much traction through the inclusion of privacy policies on websites (Yuanxiang Li, Stewart, Zhu, Ni, & Rohm Jr, 2012). A study by Case, King, and Gage (2015) indicated

that 88% of the American Fortune 500 companies now indicate how they collect PII from individuals via their privacy policies.

Although a good way to manage the risk perceptions of individuals, findings by Capistrano and Chen (2015) support earlier observations by Milne and Culnan (2004) that individuals were generally only motivated to read privacy policies to understand the extent of control they had over their data. These findings further assert that privacy concern remains a discouraging factor to information disclosure.

Organisations thus need to find new and innovative ways in reassuring individuals that their online privacy remains a priority. One avenue that could aid in this is through clearly outlining the ownership of data and the control mechanisms of access as prescribed by the RTBF principle explored in the subsequent section.

2.5. The Right to be Forgotten (RTBF)

2.5.1. Overview

The fields of information security and law has been abuzz with what has come to be known as the “right to be forgotten” (Larson, 2013; Mantelero, 2013). Despite much coverage of this new concept in the media, there seems to be no consensus on a definition for this new buzzword. Bunn (2015, p. 338) infers that the principle of being forgotten is the “right to not to be indefinitely linked to information about one's past”, a definition deduced partially from the works of Ambrose and Ausloos (2013, pp. 1-2) who define the principle as an individual’s "right to (digital) erasure" [*emphasis added*].

In 1998, Mario Costeja González sought the deletion of online records showing an outstanding social security debt he had incurred in 1998. After failing to persuade the newspaper that had published an electronic version of the article, Mr González escalated the matter to Google to have the search results to the newspaper delisted, this too proved unsuccessful. After exhausting all options, Mr González formally lodged a complaint with the Spanish data protection authority (“the AEPD”). The decision was forwarded to the CJEU, which ruled in favour of Mr González for Google to comply with the takedown request by delisting search results to the electronic article from European versions of the corporation’s search engine. The takedown request of the actual content from the newspaper was however denied. This ruling set a new precedent now known as the right to be forgotten due to the success Mr González attained (Bunn, 2015).

In light of the ruling, scholars remain perplexed regarding the full scope of the Data Protection Directive (95/46/EC) from which the CJEU based its ruling (Ustaran, 2014; Warso, 2013; Rolf H Weber, 2011). This is primarily due to the decision to keep the original newspaper content online but request Google to delist hyperlinks to the article, however, it was justified that the newspaper article was appropriate for society to be aware of the transgression. Secondly, the decision to have the hyperlinks removed from EU versions of the Google search engine has raised questions about the effectiveness of such a mechanism as it can easily be circumvented by visiting the .com (American version) of the search engine to retrieve the delisted links.

Owing to the above CJEU ruling, the RTBF principle was birthed due to the interpretation of a pre-existing law contained within the Data Protection Directive (95/46/EC) which states (Ustaran, 2014, p. 9):

- "Article 12(b) — right of rectification, erasure or blocking of data, where the processing does not comply with the provisions of the Directive;"

  Further emphasised as: "The rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data." (European Commission, 2014, p. 2)

The introduction and magnitude of the RTBF principle provides both advantages and disadvantages to individuals and society. For the purpose of this research, the assumed definition of the principle follow Ambrose and Ausloos (2013, pp. 1-2) who primarily focus on the right an individual has in requesting the erasure of personally identifiable information provided to or collected by an organisation, thus, the "right to (digital) erasure".

2.5.2. Advantages

Some advantages of the RTBF as observed from literature:

- The principle provides a "control-right" over ones data to ensure that individuals retain ownership to their data once disclosed (Ausloos, 2012)
- EU citizens can exercise this principle against an organisation in possession of their personal data where they deem that the data is inaccurate, irrelevant or excessive (European Commission, 2014)

- As per Corbett (2013, p. 247), it "allows individuals the right to control one's personal information and the right to prevent access to one's personal information"

2.5.3. Disadvantages

Some disadvantages of the RTBF as observed from literature:

- The principle has been perceived as limiting free speech, especially when compared to the American First Amendment (Larson, 2013)
- Only EU citizens can exercise this principle against an organisation (European Commission, 2014) and only if organisation has operations within the EU
- The practicality of implementing the principle have been questioned by Mayer-Schönberger (2011)

2.5.4. Aim

The fundamental aim of the RTBF principle is to eliminate EU citizens from being indefinitely associated with past transgressions within certain parameters that take into account the individual and the public's interest in the matter albeit contestation that the principle introduces a means of rewriting history (Rosen, 2012). The aura of curiosity in what this principle implies (Bunn, 2015) and its impact on non-European nations (Ambrose, 2014) have also been explored by privacy scholars.

As outlined in previous sections, breaches within social contracts have resulted in stricter measures being imposed on organisations to ensure that an individual's information is managed in a manner that is fair and transparent. One way of ensuring this is through the implementation of principles such as the RTBF, which offers individuals visibility and full control over their data from inception of its disclosure. In essence, the principle embodies what has been discussed in 2.2.3 (Social Contract Theory) by providing an exit mechanism from an established social contract through the erasure of all PII information based on an individual's request (Donaldson & Dunfee, 1994).

Indeed the RTBF principle solves largely the issue of asymmetric information (Acquisti & Grossklags, 2005), however, in light of this; it is unknown how individuals are likely to behave in future regarding the disclosure of their personal information. There is thus a need to understand not only the effect the RTBF will have on privacy and information disclosure but also the impact it will have on an individual's privacy calculus.

2.6. Conclusion

Chapter 2 covered pertinent literature regarding privacy and online information disclosure. Central to the theme of disclosure was the mental decision making process individuals undergo prior to disclosing information (privacy calculus) and the associated factors that discourage and promote such disclosures. Furthermore, key theories and concepts were introduced in Chapter 2, namely – social contract theory, the privacy calculus theory and personally identifiable information (PII). The chapter established the urgency needed for stricter privacy controls to avoid information infringements, which are a cause of privacy concern to individuals. The RTBF principle as a mechanism for individuals to have more control over their disclosed information concluded the literature review. In the subsequent chapter, an outline of the research questions distilling from the reviewed literature is provided. The associated research hypotheses that will undergo statistical testing are also outlined.

3. CHAPTER 3: RESEARCH HYPOTHESES

3.1. Introduction

A conundrum that individuals encounter frequently in an online arena is the decision to disclose or withhold personal information. Chapter 2 established that individuals face this conundrum, known as the privacy calculus, with each decision to disclose information when online. Factors which discourage and promote such information disclosure were also outlined and the principle of the right to be forgotten (RTBF) as a mechanism of providing individuals with more control over their information were deliberated.

The objectives of this research are twofold and thus this chapter outlines the research questions and hypotheses that this research aims to answer regarding the RTBF and its impact on the privacy calculus as well as information disclosure.

3.2. Research Question 1

The privacy calculus involves the user weighing out various risks and benefits associated with disclosing information online. Therefore, because the RTBF principle introduces a novel component, the following research question and hypothesis were posed to evaluate if this principle influences individuals when engaging in the privacy calculus.

RQ1: Does the RTBF influence individuals when engaging in the privacy calculus?

3.2.1. Hypothesis 1

$H1_0$: The RTBF principle does not influence individuals when engaging in the privacy calculus theory

$H1_A$: The RTBF principle does influence individuals when engaging in the privacy calculus theory

3.3. Research Question 2

Studies have shown that when the benefits outweigh the risks, individuals are more inclined to disclose personal information (Keith et al., 2013). Stemming from the previous question, it can be hypothesised that if users perceive the RTBF as a benefit when engaging in the privacy calculus, then individuals should display an increased

tendency to disclose personal information. In order to investigate this, the following research question and hypothesis were proposed:

RQ2: Does the RTBF impact individual online information disclosure?

3.3.1. Hypothesis 2

$H2_0$: The RTBF principle has no impact on individuals when disclosing online information.

$H2_A$: The RTBF principle has an impact on individuals when disclosing online information.

3.4. Conceptual Model

The conceptual module in Figure 3 details the seesaw effect that the privacy calculus has on information disclosure. Clearly depicted within this conceptual module, an increase in benefits leads individuals to increase the information disclosed based on the literature reviewed in Chapter 2. Conversely, increased perceptions of risk leads to a decrease in information disclosed. Whilst literature has comprehensively detailed the privacy calculus, the effect of the RTBF on this calculus as well as information disclosure of individuals remains unknown.

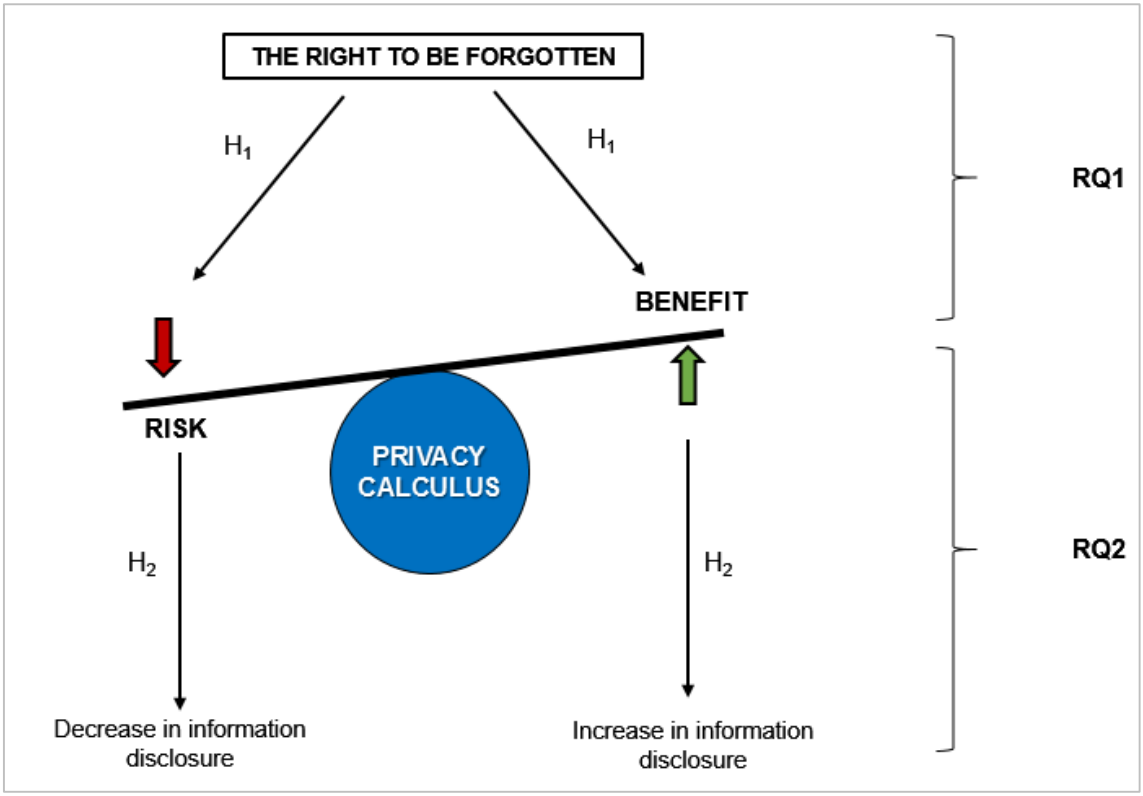

Figure 3: *Research conceptual model*
Summarises the research question with the associated hypotheses.
Source: Researcher's own construction.

3.5. Conclusion

The hypotheses highlighted above will be explored in the chapters that follow. The ensuing chapter will detail the research methodology that will be used to answer the research hypothesis mentioned in this chapter.

4. CHAPTER 4: RESEARCH METHODOLOGY

4.1. Introduction

The previous chapter outlined the research questions and associated hypotheses. Chapter 4 aims to expand and defend the choice of research methodology applied in this research to answer the stated research questions. Encompassed in the research methodology is the research design, universe, sampling, units of analysis and measurement. Each section is motivated in the context of how it was applied to answer the research questions presented in Chapter 3. The chapter is concluded with identified limitations of the research originating from insights gained after the literature review.

4.2. Research Method

A quantitative approach was employed in this research and made use of a standardised self-administered electronic survey. The approach was justified as it was the most preferred in the use of research projects which require the quantification of opinions, attitudes and the behaviours of a population in a statistical manner (Sukamolson, 2012). A deductive process was followed to ascertain “testable propositions about the relationship between two or more concepts” (Gray, 2013, p. 17) which this research aimed to achieve by evaluating the hypotheses outlined in Chapter 3. Furthermore, the methodology implemented in this research were consistent with previous research conducted by Morosan and DeFranco (2015) and Keith et al. (2013) that assessed the privacy calculus utilising various variables.

Whilst a qualitative approach could have been applied, the information gathering process of such a method often requires personal interaction in instances where focus groups or interviews are utilised. Given the nature of the research, conducting data collection using the aforementioned gathering techniques could have been construed as intrusive to the respondent’s privacy and was thus deemed inappropriate. Additionally, as illustrated in the literature review, the effect of the privacy paradox may have led to increased subject bias whereby intentions and behaviours could have been misaligned when engaged in face-to-face information gathering.

Lastly, in order to generalise the results, a large representative dataset was required. To obtain this dataset using a qualitative approach would have been extensively time-consuming. However, a quantitative approach provided a more efficient means to

obtain large dataset in a limited time and thus further motivated the selection of this method.

4.3. Research Design

The study was conducted using a descriptive research design. According to M. Saunders and Lewis (2012), descriptive designs "seek to describe accurately persons, events or situations". A descriptive design approach was deemed appropriate for this study as the researcher wanted to understand firstly, the influence of the RTBF principle (event) on individuals (persons) when engaging in the privacy calculus (situation). Secondly, the degree of impact that the privacy calculus (situation) had on individuals' (persons) information disclosure patterns in the presence of the RTBF principle (situation).

Further substantiating the use of descriptive research was the premise that extensive exploratory research had already been conducted on the topic of information privacy, disclosure and their associated trade-offs (calculus). The current study added a different dimension to the existing literary base to build upon the relationship between different factors affecting the privacy calculus in relation to information disclosure (Gray, 2013).

4.4. Population of Reference

A population needs to encompass a complete group of entities from which information can be obtained and who share common characteristics (Tustin, Ligthelm, Martins, & Van Wyk, 2005; Zikmund, Babin, Carr, & Griffin, 2012). In accordance with this, the population of this research was reasoned to be all individuals who disclosed information online and had a pre-existing online profile. For the context of this research, "online" constituted a website, portal or platform accessible on the World Wide Web through standard access techniques such as the use of a domain name, IP address or hyperlink from websites.

4.5. Sampling

4.5.1. Sampling Technique

A nonprobability sampling technique was employed in this research as it was required that participating individuals met a certain criteria in order to form part of the research population (M. Saunders & Lewis, 2012). Additionally, to obtain a list of everyone on

the Internet that disclosed information within the chosen population would not have been possible, thus affirming the usage of a nonprobability sampling technique.

Three types of nonprobability sampling were applied in this study. Purposive sampling involved selecting who would participate in the research. For this study, the motivation for purposive sampling was based on focusing on individuals who had met the population of reference, which included individuals who disclosed information online on various online platforms (Table 2). While nonprobability sampling techniques limit the generalizability to only the sample obtained (Bornstein, Jager, & Putnick, 2013), it was deemed acceptable for the research due to its cost-effective nature, ability to easily implement and ease of distribution *via* the web using a self-administered electronic survey (Fricker & Schonlau, 2002).

The purposive sampling applied the below filter to the unknown number of individuals within the population:

- **Filter 1: Individuals were required to have an online profile that was accessible via the World Wide Web**

In measuring disclosure, the study focused on individuals who disclosed information on online platforms that could potentially require exercising the principle of the RTBF to ensure erasure and removal of personal information. To limit the technicalities of this filter, a list of social networking sites were provided for selection with the option to specify “Other” alternatives in free text form. These nine sites were selected based on their popularity and feedback from peers. The nature of information disclosure mechanisms that the site afforded the user were also taken into consideration (Table 4).

Table 3: *Popular social networking sites (SNS) and disclosure mechanisms*

Type	SNS Name	Disclosure Mechanisms
Personal	Facebook	Status updates, messages, images, location
	Twitter	Status updates known as “tweets”, images
	Pinterest	Blogging and images
	Google+	Status updates, messages, images, location
	Tumblr	Images
	YouTube	Videos
	Instagram	Images
	Flickr	Images
Professional	LinkedIn	Status updates, opinion posts, education, professional affiliations, current and previous employment information

4.5.2. Sample Size

Israel (1992) and Kotrlik and Higgins (2001) recommend the use of a sample size determination table to define the appropriate sample size needed for a research. The sample size determined at a 95% confidence level and with a 5% margin of error yielded a minimum of 370 respondents. To account for possible incomplete responses, a buffer of 35% was added resulting in a target of 500 respondents required prior to terminating the survey.

4.6. Unit of Analysis

The impact on an individual's online information disclosure in the presence of the RTBF principle.

4.7. Data Collection Technique

According to M. N. K. Saunders and Bezzina (2015), research consists of systematic data collection for logical interpretation. The Internet has streamlined the data gathering processes as it supersedes traditional paper-based data collection approaches (Tustin et al., 2005). A self-administered online survey was therefore suitable for this research given that the Internet facilitates a simple and effective manner in which to obtain primary data from respondents regardless of their geographical location.

4.8. Measurement

4.8.1. Research Instrument

An online self-administered survey was conducted based on the assumption that individuals were well accustomed to using the Internet. According to Zikmund et al. (2012), Likert scales are the most well-known, easily comprehensible scales when used in surveys. The survey made use of a five-point scale ranging from "strongly agree (=1)" to "strongly disagree (=5)" as opposed to alternative scales that make use of three or seven point ranges. Motivation for the use of a five-point scale stemmed from the fact that the majority of the studies from which the questions were sourced also made use of a five-point scale. To avoid confusion amongst respondents, a decision was taken to keep a consistent scale amongst all construct questions. Included in the cover (Appendix A) of the survey were the aims and objectives of the research as well as the researcher and research supervisor's contact details should the respondent require further details. As per the University's guidelines, a confidentiality

clause was included in the cover note to ensure respondent identities were not recorded and that they were allowed to opt out at any time during the survey. The survey was hosted on the SurveyMonkey® platform.

The main advantages of an online survey include the ease of accessibility, cost and time (Denscombe, 2014; Wright, 2005). Accessibility is leveraged off the ability of the Internet to reach audiences that would otherwise be unattainable. The Internet provides an electronic medium to distribute the survey, which results in a significantly lower cost compared to paper based methods. The ease of accessibility and low cost provide an efficient way to save time as the survey can reach a large audience in a short period. Further motivators included the ease of access to the Internet given the population of reference and the convenience of allowing respondents the ability to partake in the survey from a location of their choice. Despite the value of online surveys, there are some drawbacks. These include a low response rate, ambiguity in the questions and poorly worded questions (Denscombe, 2014; Wright, 2005). The implementation of a pilot study can aid in mitigating some of the disadvantages as it can provide insight into how the survey will be perceived by the audience (M. Saunders & Lewis, 2012).

4.8.2. Research Instrument Design

The panel of questions selected for each construct in the research paper were adapted from previous research as indicated below. In cases where no suitable questions were found to address the researcher's inquiry, new questions were developed. Each section of the survey (excluding demographic data in Section A and Internet usage patterns in Section B) form part of the constructs detailed in the literature review. These constructs include:

4.8.2.1. Personal Information Sharing (Section C)

Questions regarding personal information sharing were used to assess the amount of personally identifiable information (PII) individuals were willing to disclose online. These questions were adapted from previous research conducted by Fogel and Nehmad (2009). A new question (Q11.12; Appendix B) was developed to assess whether individuals try to conceal their identity by creating alternative personas when online. All questions in this section consisted of "Yes" or "No" answers.

4.8.2.2. Privacy Concern (Section D)

Questions in this section were adapted from Dinev and Hart (2006) and Joinson et al. (2010). They were aimed at assessing how concerned individuals were regarding their

privacy. New questions (Q12.2, Q12.5, Q12.7, Q12.8; Appendix B) were developed to assess whether privacy concern extended to the physical concern of being found due to PII disclosed online and to gauge the level of concern regarding the retention of data by organisations.

4.8.2.3. Need for Awareness (Section E)

Questions in this section were developed to assess the level of awareness of individuals regarding how their information is utilised and how much more they would like to increase this awareness. Questions were adapted from research conducted by Malhotra et al. (2004). Newly developed questions (Q13.1, Q13.2, Q13.3, Q13.5; Appendix B) regarding awareness of privacy policies and usage of privacy filters were inspired by Wu et al. (2012).

4.8.2.4. Lack of Perceived Control (Section F)

Central to the theme of privacy is the level of perceived control the user is believed to have over their data (Aaron Gabisch & R. Milne, 2014). To assess how much control individuals perceived to possess over their information, questions were adapted from Doherty and Lang (2014). The measurement scale was reduced from a 7-point Likert to a 5-point Likert ranging from “no control at all (=1)” to “complete control (=5)”.

4.8.2.5. Privacy Scenarios (Section G, Section H and Section I)

The three privacy scenarios were adapted from Malhotra et al. (2004) based on their Scenario Type A (STA), regarding individual’s willingness to supply less sensitive information and, Scenario Type B (STB) requesting more sensitive information. Privacy scenario 1 (PS1) and privacy scenario 3 (PS3) were based on STA and STB respectively. Privacy scenario 2 (PS2, Q16; Appendix B) removed the monetary incentive provided in the other scenarios to assess whether intention to disclose information would be affected if the RTBF principle substituted the economic gain offered to the individual.

4.8.2.6. Perceived Benefits (Section J)

Questions regarding perceived benefits were adapted from H. Xu et al. (2011). These questions were used to gauge what individuals consider as benefits in using the hypothetical website presented in the various privacy scenarios.

4.8.2.7. Trust (Section K)

The hypothetical website in the privacy scenarios requested personal information about the individual, work related information, information about their friends and family as well as their financial position. Thus, an understanding of how trust in the website was affected by the different variables was required. To address this, questions were adapted from H. Xu et al. (2011). New questions (Q18.5, Q18.8, Q18.9; Appendix B) regarding the erasure of passively provided information were based on the works of Bunn (2015).

4.8.3. Research Instrument Pre-Testing

The pilot survey took place from 5 August 2015 to 12 August 2015 and comprised of 19 randomly selected respondents who were asked to complete the survey. Individuals were conveniently sampled from the researcher's MBA class and within the researcher's company, which included colleagues and directors. The demographic data and reliability scores (Appendix C) indicated that the survey was suitable to be widely distributed following a few amendments.

Respondents were asked to offer suggestions and recommendations on how the survey could be improved. Feedback from the survey was favourable and valid comments regarding the questions, sequence, scale and layouts were obtained. In particular, a few respondents observed that, considering most individuals make use of mobile phones, the layout needed to be adaptive to devices such as smartphones and tablets. To accommodate these devices, adjustments were made to the visual settings on the survey tool and tested by the researcher. Most notably, the survey was perceived to be too lengthy (extending over 20 pages), so further logical grouping of questions and renaming of the constructs were done on the survey tool. These changes were incorporated into the final survey (Appendix B).

The majority of the respondents provided feedback that the survey made them cognisant about their online conduct and how much information they actually disclosed. This generated a multitude of topical discussions amongst members of the executive committee in the researcher's company. Most executives expressed concern about how privacy awareness should be a core focus in training owing to the sensitive nature of the business. Stemming from this, the CEO authorised the distribution of the survey to the organisation's entire mailing list. It was envisioned that the results of the survey would yield much needed guidance to how training regarding online privacy should be structured within the organisation.

Overall, there were no constraints experienced during the pilot of the survey instruments. It was noticeable that respondents were taking longer than the 10 minutes specified on the consent page; however, the time was kept the same as the respondents could have been disrupted whilst completing the survey for various reasons. During the pilot, it became apparent that the survey tool had the ability to record the IP addresses of respondents in order to categorise them. An IP address can be classified as a form of personally identifiable information as it can be used to identify the location of respondents, thus making it less anonymous in nature. The feature was turned off for the final survey to avoid recording any PII about the user or their location.

4.9. Data Integrity

Data integrity refers to the accuracy and consistency of the data collected during the final survey. It is necessary to ensure that no changes are made to the data from the time it is received until the time it is processed. Once the raw data has been collected, it is subsequently processed through data editing and data coding to transform the data into useful information. Data integrity needs to be maintained through all of these steps to avoid generating errors (Zikmund et al., 2012).

4.10. Data Editing

To ensure that the response data obtained in the final survey was consistent and did not include any omission or errors, data editing was performed to groom the data for statistical analysis (Zikmund et al., 2012). The procedures required to edit the data included rectifying missing data and ensuring that the responses were correctly coded.

4.10.1. Missing Data

When performing a survey, missing data arises when respondents do not answer all of the questions (Uma & Roger, 2003). These could be for a number of reasons, including:

- Ambiguity of the question
- Unwillingness to answer the question
- The individual may not know how to answer the question

Missing data can be processed in a two-fold manner – firstly, the type of missing data needs to be identified and secondly the appropriate technique to rectify the data needs to be selected (Cooper & Schindler, 2013). There are three types of missing data and three techniques to rectify the data:

Types of missing data:

- Missing completely at random (MCAR)
- Missing at random (MAR)
- Missing not at random (MNAR)

Types of correction techniques:

- Listwise deletion
- Pairwise deletion
- Predictive replacement

The type of missing data and the corresponding correction technique was assessed upon completion of the survey.

4.10.2. Data Coding

Data coding refers to the process of assigning numbers and other symbols to previously edited data so that one can classify the responses into categories (Cooper & Schindler, 2013; Zikmund et al., 2012) and was performed following the removal of missing data. Categories need to be appropriate to the research problem and designed carefully to maximise the information that can be obtained from the data. When performing a survey using an online tool such as SurveyMonkey®, universal coding rules are already embedded in the software to prevent any issues when coding the data, e.g. human error of coding a response as a three instead of a two. However, in some cases, the data needed to be recoded and this was performed through data transformation.

4.10.3. Data Transformation

Three data transformations where performed in this research, the justifications of which are provided below. The first data transformation performed was recoding the original code embedded in SurveyMonkey®, into another value (Sekaran & Bougie, 2010). This was done to avoid any problems that could arise in downstream analyses. Recoding were applied to the data collected for Section C, which related to the individuals online profiles and PII information the individual was willing to disclose.

For Question 10, the data was recoded based on the number of online profiles an individual selected. These were categorised as follows:

- Low online presence (≤ 3 profiles)

- Medium online presence (4 – 5 profiles)
- High online presence (>5 profiles)

For Question 11, the data was recoded based on the extent of an individual's PII disclosure and was categorised as follows:

- Low degree of information disclosure (≤ 3 "yes" answers)
- Medium degree of information disclosure (4 – 6 "yes" answers)
- High degree of information disclosure (>6 "yes" answers)

The more questions answered "yes", the higher the level of PII disclosure. This method of recoding was appropriate because it was the best partitioning of the data for testing hypotheses and showing relationships.

The second type of data transformation applied was reverse scoring. Within a scale, if you have some statements indicating high agreement as a positive outcome, and other statements indicating high agreement as a negative outcome, the meaning of some of the responses will require reverse scoring to maintain consistency (Sekaran & Bougie, 2010). In other words, certain statements would be required to be reverse scored to ensure that high agreement consistently indicated only a positive outcome, or only a negative outcome. Reverse scoring was applied (Q18.3, Q18.4; Appendix B) to maintain that high levels of agreement measured a positive outcome.

The final type of data transformation applied was condensing several questions that measured the same concept and was executed by combining the scores of the original questions into a single score (Sekaran & Bougie, 2010). In this study, composite measures were created by averaging all related variables for the following measure scales:

- Privacy Concern
- Need for Awareness
- Lack of Perceived Control
- Trust
- Perceived Benefits
- The privacy scenarios (Scenario 1 – 3)

4.11. Analysis Approach

4.11.1. Scale Reliability and Validity

The data generated from the survey were tested for reliability and validity before any statistical tests (Spearman's Correlation, Kruskal Wallis and Mann-Whitney U) were conducted. This was done to ensure that the data was valid and usable to answer the research questions posed. The reliability scores were used to indicate the consistency in which the data was collected. According to M. Saunders and Lewis (2012, p. 128) reliability can be defined as "the extent to which data collection methods and analysis procedures will produce consistent findings". In this study, the reliability scores were used as a way to measure that the individual items in the survey produced consistent results.

According to Uma and Roger (2003), the reliability of a measure is established by testing for both consistency and stability. Consistency is indicative of the collective strength of a group of items measuring a single concept. The most common statistical index used to measure reliability is the Cronbach's alpha, which measures the reliability coefficient and therefore indicates the correlation between items in a set. Cronbach's alpha is computed in terms of the average inter-correlations among the items measuring the concept. Generally, reliabilities with a Cronbach's alpha of at least 0.7 are acceptable, whereas 0.6 is considered poor and 0.8 is regarded as good (Uma & Roger, 2003). For the purposes of this study, Cronbach's alpha were computed for all measurement scales, namely privacy concern, need for awareness, lack of perceived control, trust, perceived benefits and the three privacy scenarios.

However, reliability does not indicate validity. The fact that an item was measured consistently does not mean that the correct factor was being measured. According to M. Saunders and Lewis (2012, p. 127), validity is defined as "the extent to which data collection method or methods accurately measure what they were intended to measure; and additionally as the extent to which research findings are really about what they profess to be about". There are several types of validity, with the most common ones including content validity, factorial validity, construct validity, criterion validity and face validity (M. Saunders & Lewis, 2012). Content validity is used to validate that the questions posed in the survey accurately reflect the research objectives that have been outlined (M. Saunders & Lewis, 2012). There are two ways to achieve this:

- The questions should be based on solid literature and

- Using a panel of individuals to assess if the questions are effective and useful.

Related to content validity is factorial validity, which refers to clustering the correlations of the respondents by creating groups. Factorial validity can be measured by performing a principle component factor analysis that will assess if the dimensions that were posed in theory emerge as true dimensions (Uma & Roger, 2003). A factor analysis also reveals whether the theoretical dimensions (i.e. constructs) are indeed tapped by the items in the measure, as theorised.

Construct validity refers to "the extent to which your measurement questions actually measure the presence of those constructs you intended them to measure" (M. Saunders & Lewis, 2012, p. 142), and criterion-related validity is concerned with "the ability of the measures (questions) to make accurate predictions" (M. Saunders & Lewis, 2012). Face validity is when "a question and its measurement criteria appears to be rational in reflecting accurateness in what is intended to be measured" (M. Saunders & Lewis, 2012).

For the purposes of this study, all measurement scales were subject to principal component factor analysis. Included in the principle component analysis is the requirement to assess the worthiness of the factor analysis. This was done by measuring the Kaiser-Meyer-Olkin (KMO) index and the Bartlett's test of sphericity. A KMO index of greater than 0.5 is deemed acceptable and the Bartlett's test should be significant at least at the 95% confidence level. Further analyses of the factor loadings were used to compute composite construct reliability (CCR) and average variance extracted (AVE). A scale is considered to demonstrate adequate reliability and construct validity if CCR is above 0.7 and AVE is greater than 0.5 (H. Li et al., 2011). All measurement scales that were found to be reliable were used to create composite scores by averaging all the variables within each construct. These composite scores, in the form of averages, were then used to conduct the correlation analysis and statistical analyses (M. Saunders & Lewis, 2012).

4.11.2. Correlation Analysis

A correlation coefficient, represented by the letter "ρ", is a statistical method that allows for the linear relationship between two variables to be quantified (M. Saunders & Lewis, 2012). The Spearman's correlation coefficient test was selected for this study due to the fact that such a test helps assess the "strength of the relationship between two variables and the probability of this occurring by chance" if the data is categorically ranked according to M. Saunders and Lewis (2012, p. 180). Thus, for the purposes of

this study, Spearman's correlation coefficient was used to assess the strength of relationship between all the constructs (privacy concern, need for awareness, lack of perceived control, trust, perceived benefits) in relation to each of the three privacy scenarios.

The strength of the relationship is determined by a value ranging between -1 and +1, with values closer to +1 representing a very strong positive correlation and values closer to -1 representing a very strong negative correlation which is graphically represented in Figure 4 below.

Figure 4: *Values of the correlation coefficient.*
Source: M. Saunders and Lewis (2012, p. 183).

A positive correlation signifies that the two variables are dependent on each other i.e. an increase in the one variable will result in an increase in the other variable whist the opposite is valid for a negative correlation. A value of zero (0) indicates that the two variables are perfectly independent of one another.

4.11.3. Statistical Validation

A Kruskal Wallis one-way analysis of variance is a statistical test applied when data is collected on an ordinal scale is most appropriate when there is a random selection independence in the samples (Cooper & Schindler, 2013, p. 460). The Kruskal Wallis one-way analysis of variance test was conducted in which each privacy scenario was directly compared to information disclosure, i.e. Privacy scenario 1 vs. information disclosure, privacy scenario 2 vs. information disclosure and privacy scenario 3 vs information disclosure.

The Mann-Whitney U test was used to compare two independent samples when the data is ordinal (Cooper & Schindler, 2013, p. 615). Information disclosure was subdivided into three categories (low, medium and high) which refers to the degree of disclosure an individual has. The Mann-Whitney U test was applied to determine the significance between each category, i.e. low information disclosure vs. medium disclosure, low information disclosure vs. high information disclosure, and medium

information disclosure vs. high information disclosure in relation to the three privacy scenarios

4.12. Limitations

Whilst the study at hand can provide valuable insight into the evolving concept of privacy, it does have some limitations. Firstly, the intricacies of the RTBF principle are not fully explored within the context of this study; rather focus was only given to the erasure request of individuals who opted to have their personal information erased ("forgotten"). In so doing, many assumptions were made which extended the principle to not just data providers such as Google and other search engines, but all organisations – this is currently not how the judgement by the CJEU is implemented (Rolf H Weber, 2011).

Secondly, the privacy calculus was used as a base theory however, upon further research in the arena of privacy, alternative theories such as the Theory of Planned Behaviour (TPB) and Theory of Reasoned Action (TRA) may have been suitable alternatives to the study as these theories aim to understand perceived behavioural control and how it is influenced by behavioural intent (Ajzen, 1991).

Thirdly, the constructs selected for this study were based on various studies regarding privacy concern, disclosure and control to apply against the privacy calculus. Whilst these constructs cover those most commonly used in literature, other constructs that were not investigated could have added more insight into the RTBF principle. Lastly, though the results of this study may shed light on the behavioural factors affecting individuals in the presence of the RTBF principle, no technical frameworks or implementation recommendations were provided. This study mainly focused on empirical data, however, organisations could benefit from studies that investigate the implementations of the findings contained herein.

4.13. Conclusion

A quantitative method was applied to determine the impact the RTBF principle had on the privacy calculus and information disclosure. The study was descriptive in nature and employed the use of an online survey to collect data. A pilot study was conducted to pre-test how the survey would be perceived by the audience. The appropriate modifications were made to the final survey and a nonprobability sampling technique was applied. Editing and transformation of the data were performed prior to the statistical analyses performed. The subsequent chapter discusses the results obtained

from the survey and the statistical tests in an attempt to answer the research questions of the study.

5. CHAPTER 5: RESULTS

5.1. Introduction

An online survey was used to obtain information from individuals regarding how the RTBF principle influenced their decision to disclose personal information online. The electronic survey (Appendix B) was distributed on Thursday 17 August 2015 and disabled on 3 September 2015 after the expected target of respondents was achieved.

The aim of this chapter is to present the results of the survey beginning with how the data was edited and the descriptive statistics of the respondents. Following on from this, the reliability and validity results of the survey are presented. The statistical tests outlined in Chapter 4 were used to answer the research questions posed in Chapter 3 and the outcome of these results are presented. The chapter is concluded with the statistical findings per hypothesis.

5.2. Data Editing

Data editing is a process that grooms the data obtained from the survey for statistical analyses by ensuring that all errors are filtered out and was performed in this study as follows:

- The responses (502) were extracted from the SurveyMonkey® database. Each response was automatically coded and assigned a numerical response ID.
- The data was processed to remove the partially completed responses (66) thus making the data more complete and consistent.
- The responses were further screened to ensure that the respondents fell within the sampling frame of having an online profile. An additional six responses were excluded based on this criterion.

At the end of the data editing process, 430 responses remained. These responses were then evaluated for missing data.

5.2.1.1. Missing Data

It was established that this study contained MCAR as the type of missing data. When performing a survey, an MCAR event occurs when an individual skips over a question for no apparent reason i.e. the reason was random. The approach best suited to correct for MCAR is listwise deletion, which completely excludes the data if a variable

is missing. Listwise deletion was performed automatically in this study, using IBM's Statistical Package for the Social Sciences (SPSS).

The best option to process a blank response is to ignore the entry and is the default option in most statistical programs (Uma & Roger, 2003). An advantage of analysing the data in this manner was that only fully completed responses were included thereby avoiding any bias. However, the disadvantage of this approach was that it could cause a reduction in the sample size. The large number of respondents (> 500) in this study allowed for blank responses to be deleted without affecting any relationships between the variables being investigated.

In addition to the listwise deletion, the data was further manually filtered. This was performed in cases where an individual selected "other" when choosing between the social network platforms but did not have a valid alternative. Processing the data automatically and manually produced the most complete, consistent and readable information that could be used to conduct the statistical analyses, which resulted in 389 responses.

5.3. Descriptive Statistics

The demographic profiles of the respondents that participated in the final survey are illustrated below.

5.3.1. Characteristics of Respondents

Majority of the respondents that participated in the survey were between the ages of 25 and 45 (Figure 5). Individuals within these age groups are generally users of SNS and are inherently more likely to disclose information when online.

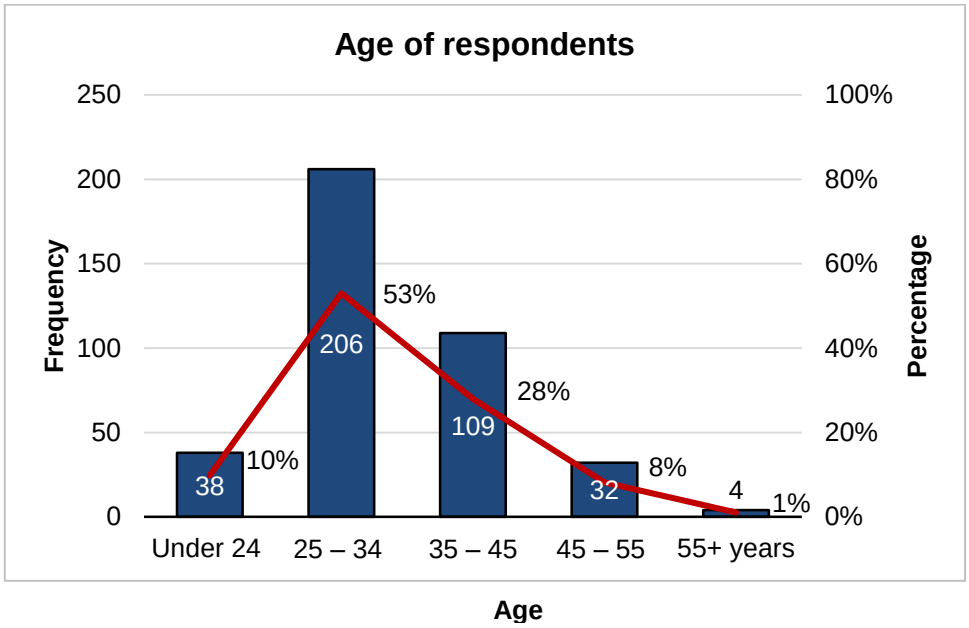

Figure 5: *Age of respondents.*
The x-axis represents the different age classes. The left y-axis indicates the number of respondents in each category and the right y-axis indicates the relative percentage to the total number of respondents.

There was no gender bias observed amongst the respondents as indicated in Figure 6. The sampled population was diverse and represented individuals from various different ethnicities (Figure 7) however, as shown in Figure 8, the population was primarily composed of individuals from South Africa. Therefore, the findings of this study cannot be generalised for a global population.

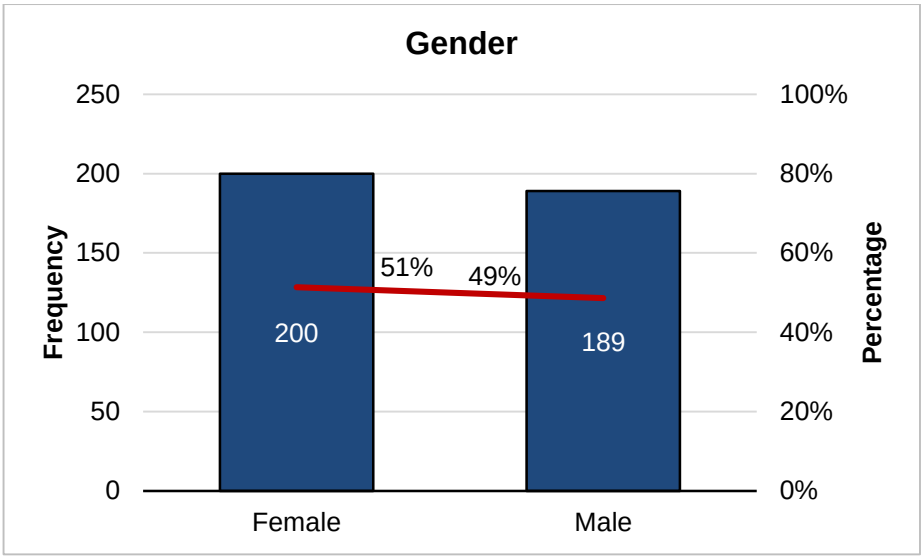

Figure 6: *Gender distribution amongst respondents*

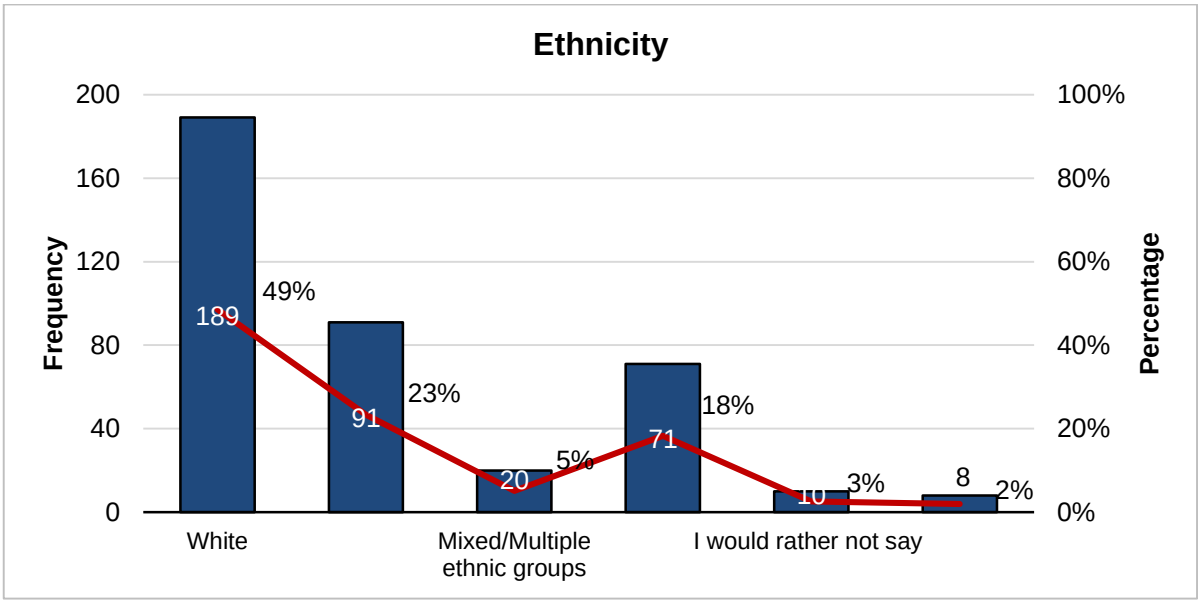

Figure 7: *Ethnicity of respondents.*
The left y-axis indicates the number of respondents in each category and the right y-axis indicates the relative percentage to the total number of respondents.

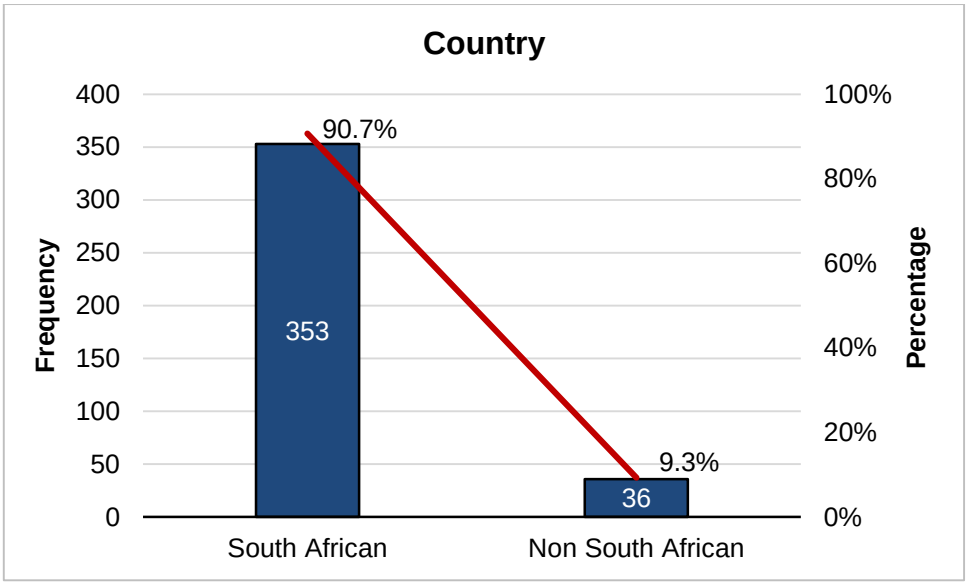

Figure 8: *Country of origin of respondents.*
The left y-axis indicates the number of respondents in each category and the right y-axis indicates the relative percentage to the total number of respondents.

The majority of respondents had extensive experience in Internet usage, most exceeding a tenure of 10 years (Figure 9). Increased Internet usage may also be indicative of more time to disclose information online. Figure 10 illustrates the devices used most frequently by individuals to access the Internet. Mobile alternatives such as smartphones, IPads and tablets were used more frequently than traditional desktops or laptop computers (whether private or company owned). The average time spent online by respondents ranged between one to six hours per day as depicted in Figure 11. This may be justifiable given the attachment individuals have developed over time to smartphones and tablets.

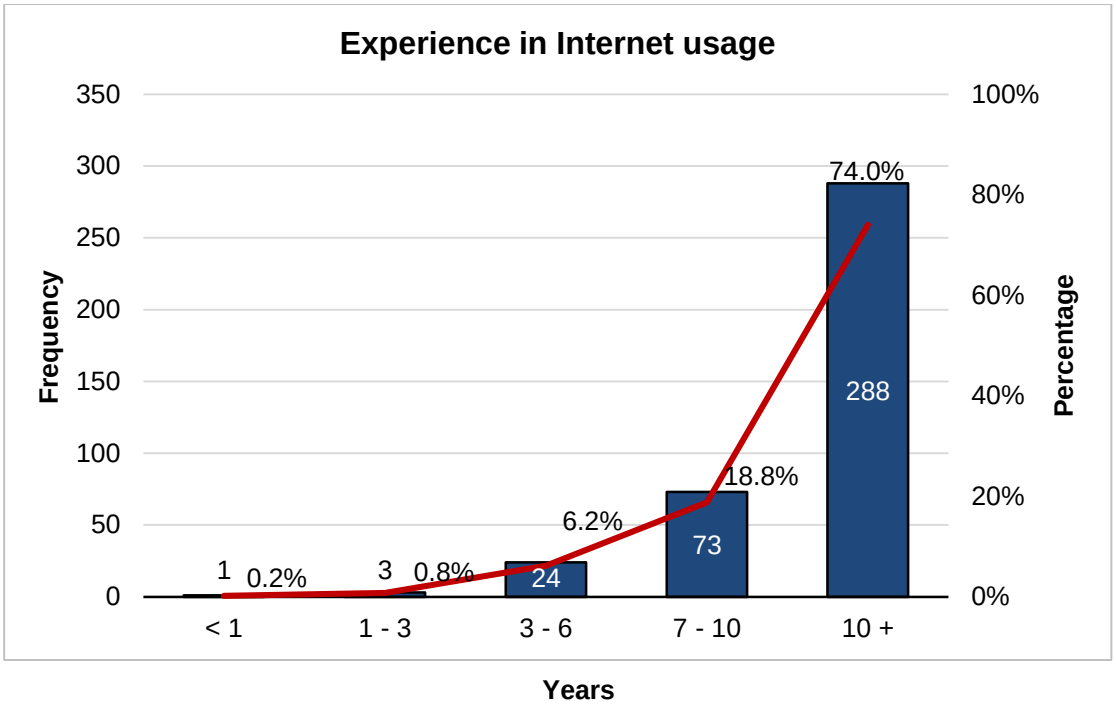

Figure 9: *Internet usage experience indicated by respondents. The x-axis represents the years of experience. The left y-axis indicates the number of respondents in each category and the right y-axis indicates the relative percentage to the total number of respondents.*

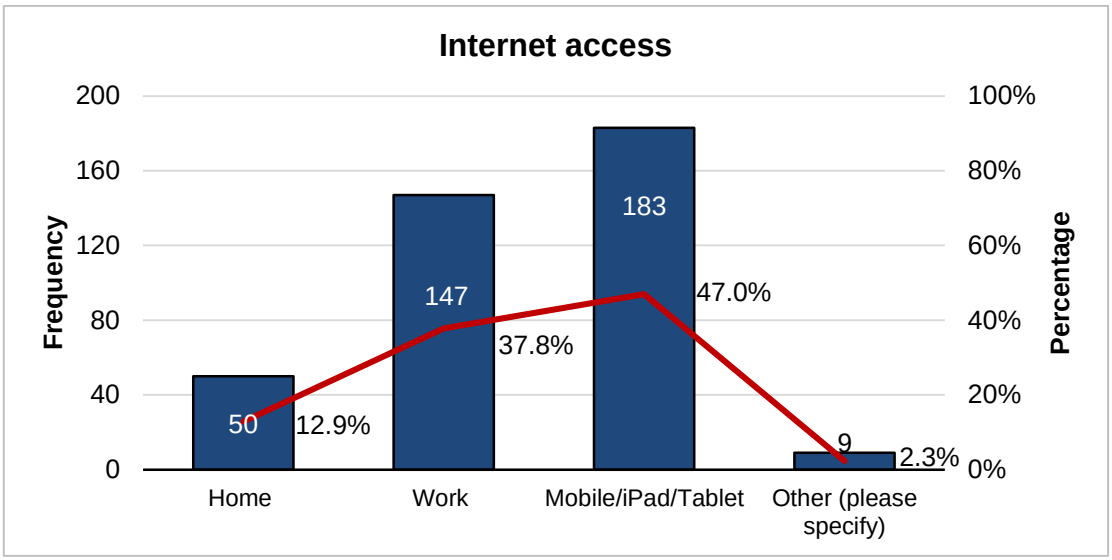

Figure 10: *Internet usage devices used by respondents. The left y-axis indicates the number of respondents in each category and the right y-axis indicates the relative percentage to the total number of respondents*

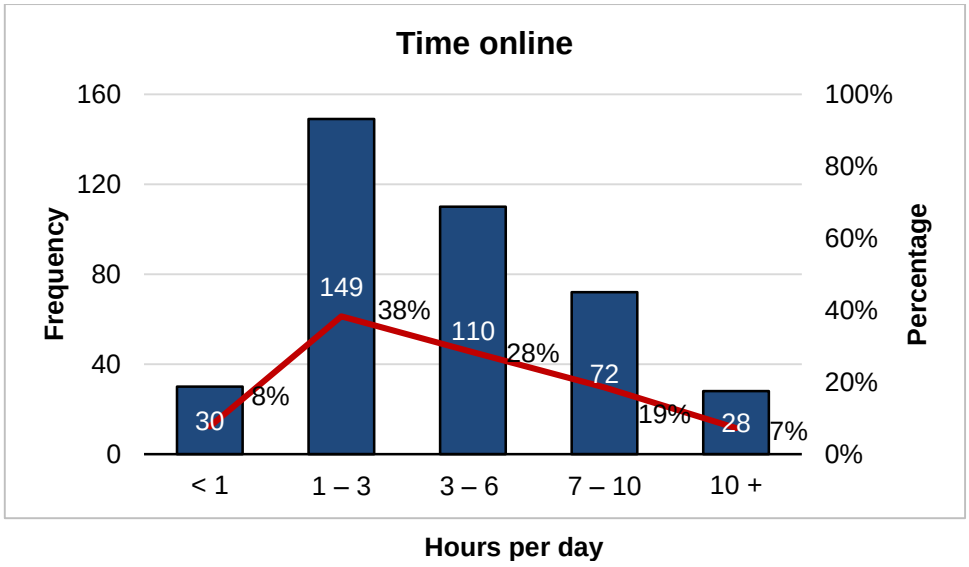

Figure 11: *Average time spent online by respondents.*
The x-axis represents the hours per day spent online by individuals. The left y-axis indicates the number of respondents in each category and the right y-axis indicates the relative percentage to the total number of respondents.

The SNS platform that was most popular amongst the respondents was Facebook (Figure 12). Facebook, which boasts more than 1.5 billion users was followed by LinkedIn, which despite a lower user base (380 million users), is more used for professional engagement with colleagues within and outside of an individual's company.

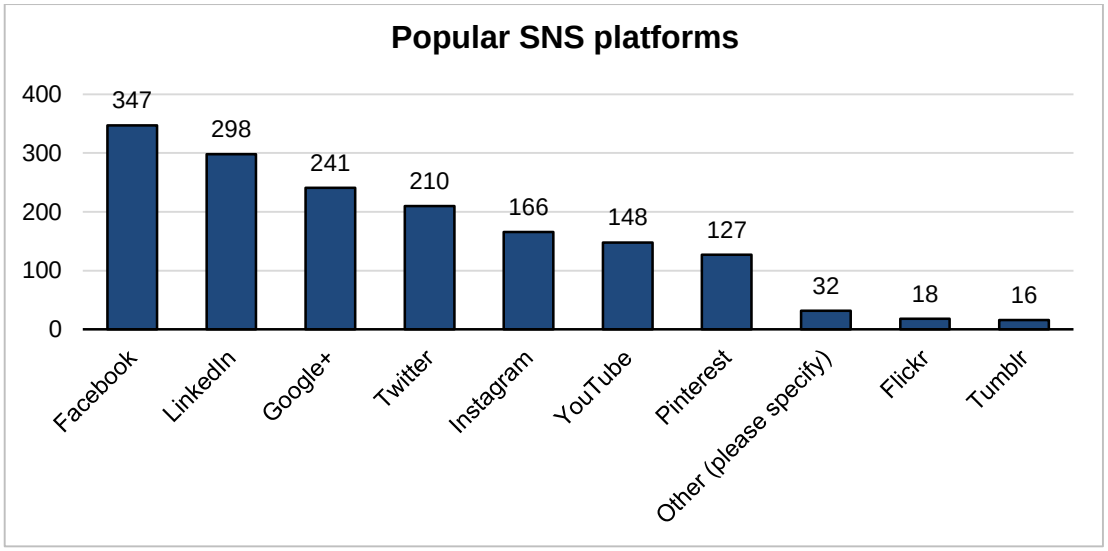

Figure 12: *Popularity of SNS platforms amongst respondents. The x-axis represents the various SNS platforms. The y-axis represents the number of respondents how indicated having a profile on the SNS.*

The number of SNS profiles that were held by the respondents were used to categorise the individuals into groups of low online presence (≤ 3 profiles), medium online presence (4 - 5 profiles) and high online presence (> 5 profiles). The majority of respondents had a low online presence whilst a relatively large amount of respondents had a medium online presence (Figure 13). This may be attributed to the fact that SNS generally cater for very specific functions (such as personal sharing, professional, hobby, etc.).

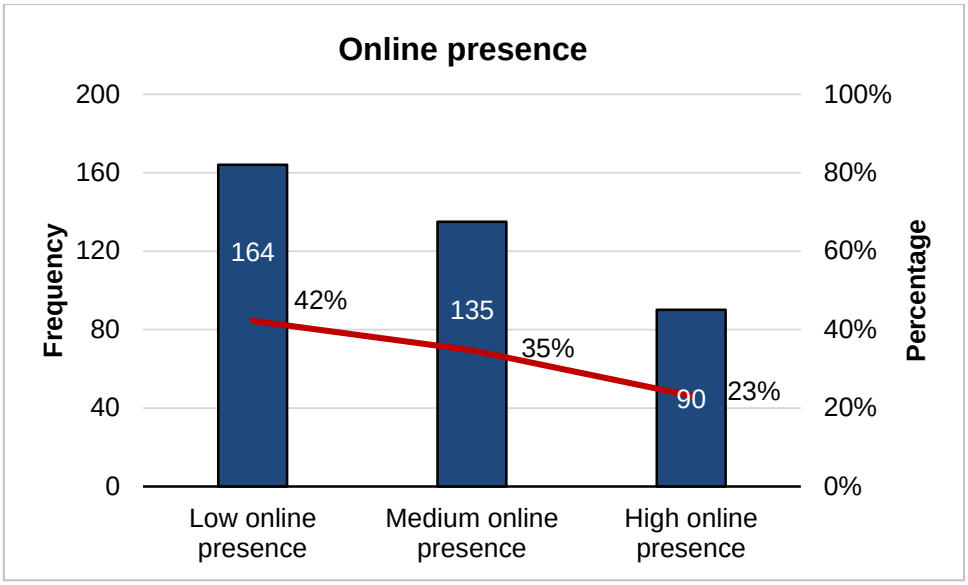

Figure 13: *Number of profiles held by the respondents. The left y-axis indicates the number of respondents in each category and the right y-axis indicates the relative percentage to the total number of respondents.*

In addition to online presence, the respondents were categorised based on the extent to which an individual disclosed personal information online and was determined on the number of "yes" answers selected in question 11. Individuals were divided into low degree of information disclosure (≤ 3 "yes" answers), medium degree of information disclosure (4 – 6 "yes" answers) and high degree of information disclosure (>6 "yes" answers). The majority of respondents were in the category of medium degree of information disclosure (Figure 14). Given the polar differences between low degree of information disclosure and high degree of information disclosure, the results should present interesting outcomes on whether indeed their behaviours online align to their views.

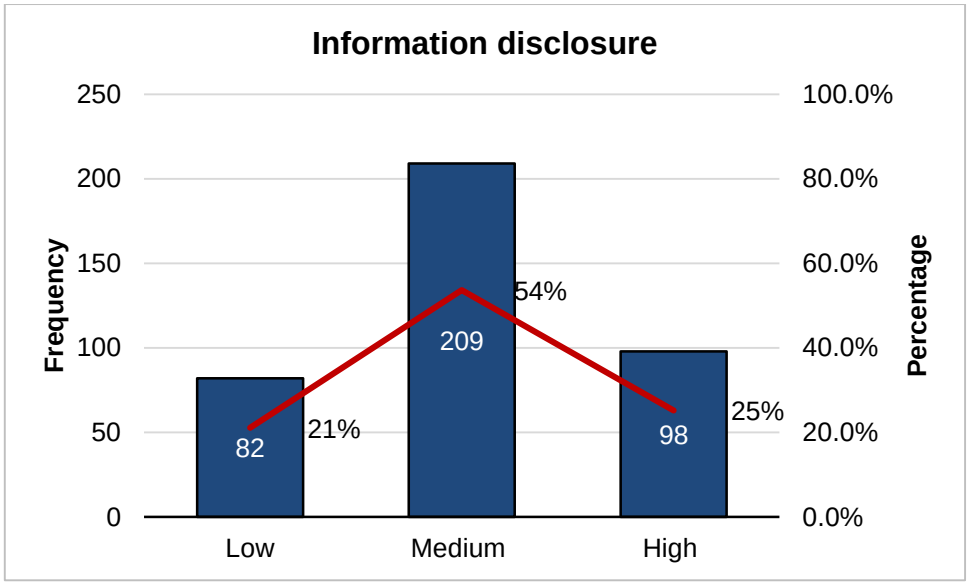

Figure 14: *Information disclosure categories.*
Based on data transformation performed on respondents based on the degree of personal information they are willing to disclose

The demographic statistical results indicate that a diverse population was sampled representing individuals with different levels of online information disclosure from across a broad number of ethnicities and age. A table summary of the demographic data is shown in Appendix D. Whilst the results may only be applicable in the context of South Africa, this population can be used to assess the impact of the RTBF principle with regard to the privacy calculus. The subsequent sections will evaluate results obtained for the different components of the survey and their impact on the privacy calculus.

5.4. Results per Privacy Calculus Construct

The results below summarise what was observed for the various measurements examined in the survey. These include the constructs relating to the privacy calculus (privacy concerns, the need for awareness, the lack of perceived control, perceived benefits and trust) and three different scenarios influencing an individuals' privacy consideration. The central tendency statistics results for each construct can be found in Appendix E.

5.4.1. Privacy Concern

An individuals' privacy concern was evaluated using the questions indicated in Table 4. In Figure 15, the level of concern with statements pertaining to the individuals' privacy are depicted. Most predominantly, respondents showed increased concern regarding information misuse on the Internet (**PC1** and **PC6**).

Table 4: *Questions regarding privacy concern of individuals*

	Question
PC 1	I am concerned that the information I submit on the Internet could be misused
PC 2	I am concerned that a person can find personal information about me on the Internet
PC 3	I am concerned about submitting information on the Internet because of what others might do with it
PC 4	I am concerned about online identity theft
PC 5	I am concerned that organisations may keep my information for longer than I anticipate
PC 6	I am concerned about submitting information on the Internet because it could be used in a way I did not foresee
PC 7	I am concerned that online companies are collecting too much personal information about me
PC 8	I am concerned about threats to my personal privacy

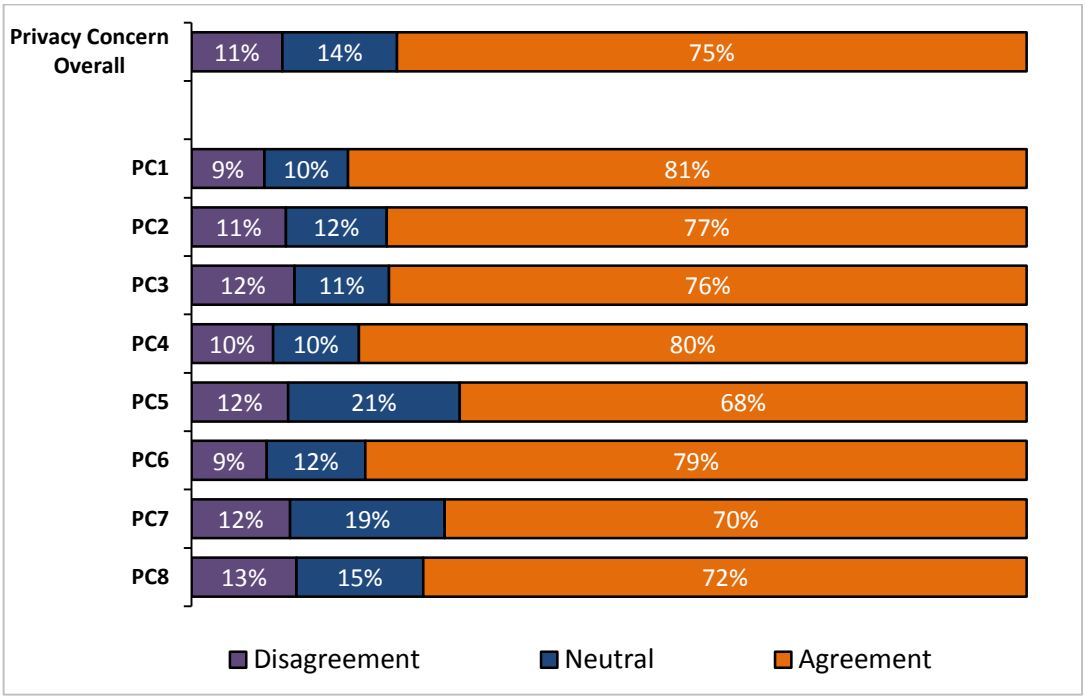

Figure 15: *Concern individuals have regarding their privacy*.

5.4.2. Need for Awareness

The need for awareness individuals require over their personal information was assessed with the questions in Table 5. In general, it was observed that individuals have a high need for awareness regarding the usage and distribution of their information (Figure 16). Despite their need for awareness, very few respondents indicated that they read privacy policies (**Aware 4**) before registering for an online service, which appears to contradict their need for awareness.

Table 5: *Questions regarding need for awareness*

	Question
Aware 1	Companies seeking personal information online should disclose the way the data is collected, processed and used
Aware 2	A good privacy policy should have a clear and conspicuous disclosure
Aware 3	It is very important to me that I am aware and knowledgeable about how my personal information is used
Aware 4	I always read the privacy policy before registering for an online service
Aware 5	I always make use of privacy filters to control who can see certain details on my online profile(s)

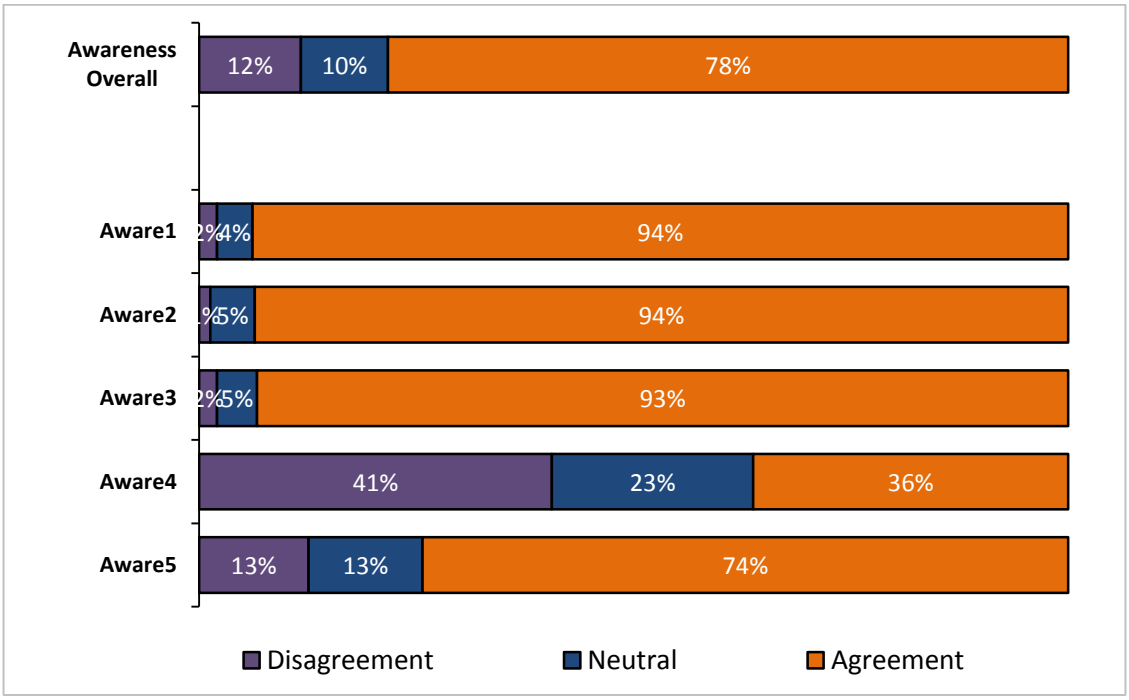

Figure 16: *The need of awareness regarding personal information.*

5.4.3. Lack of Perceived Control

The level of control that individuals perceive to have over their information was evaluated with the questions in Table 6. Individuals generally did not perceive to have much control over the information they submit online (Figure 17). Inherent to this is the fear that inaccurate information about them cannot be easily corrected (**Control 2**) and inability to prevent unwanted analysis of their data (**Control 5**).

Table 6: *Questions regarding lack of perceived control*

	Question
Control 1	Your ability to control who can view your information
Control 2	Your ability to control the actions of other online users
Control 3	Your ability to correct inaccurate or untruthful information about yourself
Control 4	Your ability to remove embarrassing or damaging information about yourself
Control 5	Your ability to prevent your data and actions from being used/analyzed by online companies in ways that you did not intend
Control 6	Your ability to prevent your data and actions from being used/analyzed by other parties in ways that you did not intend

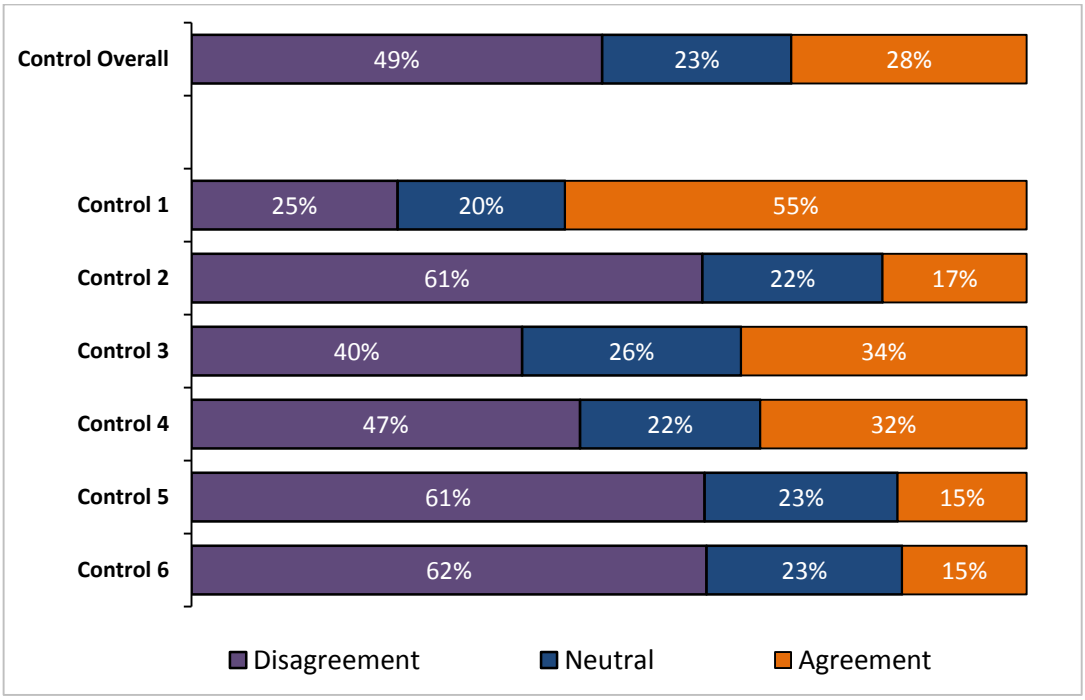

Figure 17: *Level of perceived control.*
Constructs relating to the level of control individual's perceive they have over how their personal information is used online.

5.4.4. Perceived Benefits

In the preceding results, the three scenarios were evaluated independently. The results below illustrate the influence that perceived benefits (Table 7) had on information disclosure in relation to all three scenarios. In Figure 18, individuals were shown to be more likely to provide personal information in relation to the three scenarios in cases where the website provided individuals the convenience to access information (**Benefit 1**), and when the website provided them with additional benefits (**Benefit 2**).

Table 7: *Questions regarding perceived benefits*

	Question
Benefits 1	The website provides me with the convenience to instantly access the information I need
Benefits 2	Overall I feel that using the website is beneficial

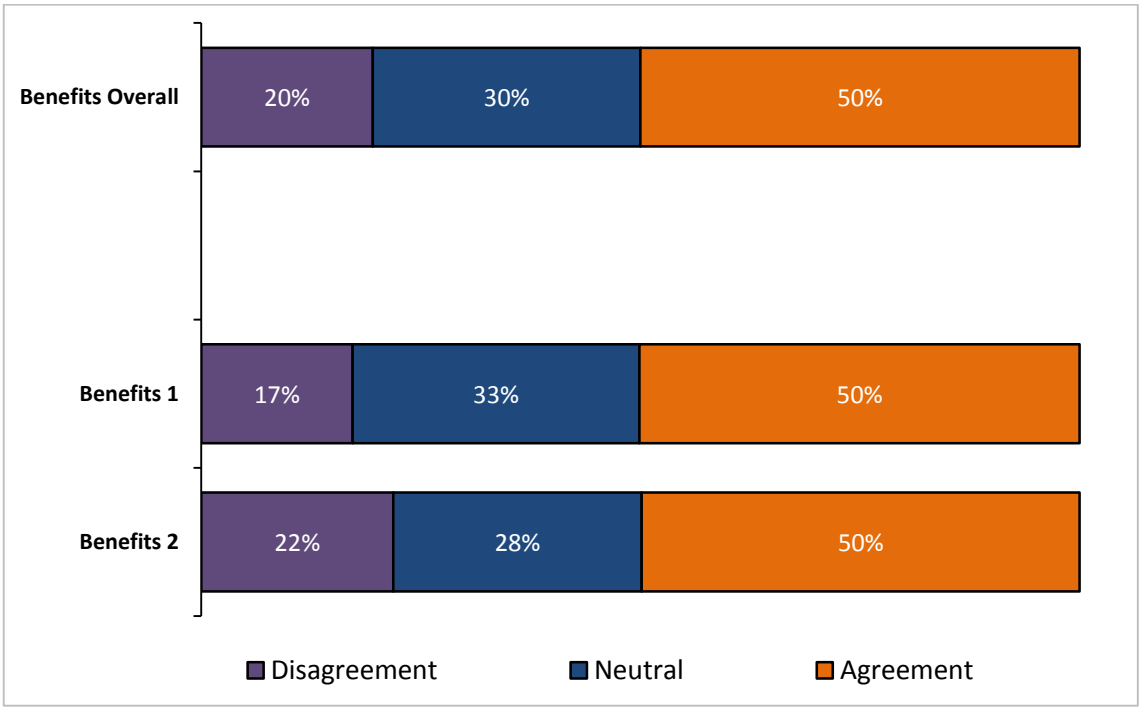

Figure 18: *Perceived benefits.*
Construct depicting the effect that perceived benefit has on information disclosure in relation to the three scenarios.

5.4.5. Trust

The three scenarios were used to investigate the level of trust that individuals have on the website to which they are required to disclose information (Table 8). Figure 19 shows that overall individuals did not show trust towards the website in relation to the three scenarios provide to them.

Table 8: *Questions regarding trust*

	Question
Trust 1	I am aware that providing the website with my personal information may involve experiencing unexpected problems
Trust 2	It would be risky to disclose my personal information to the website
Trust 3	Overall, I see no real threat to my privacy by disclosing personal information to the website
Trust 4	I think my benefits gained from using the website can offset the risks of my information disclosure
Trust 5	The value I gain from using the website is worth the information I give away

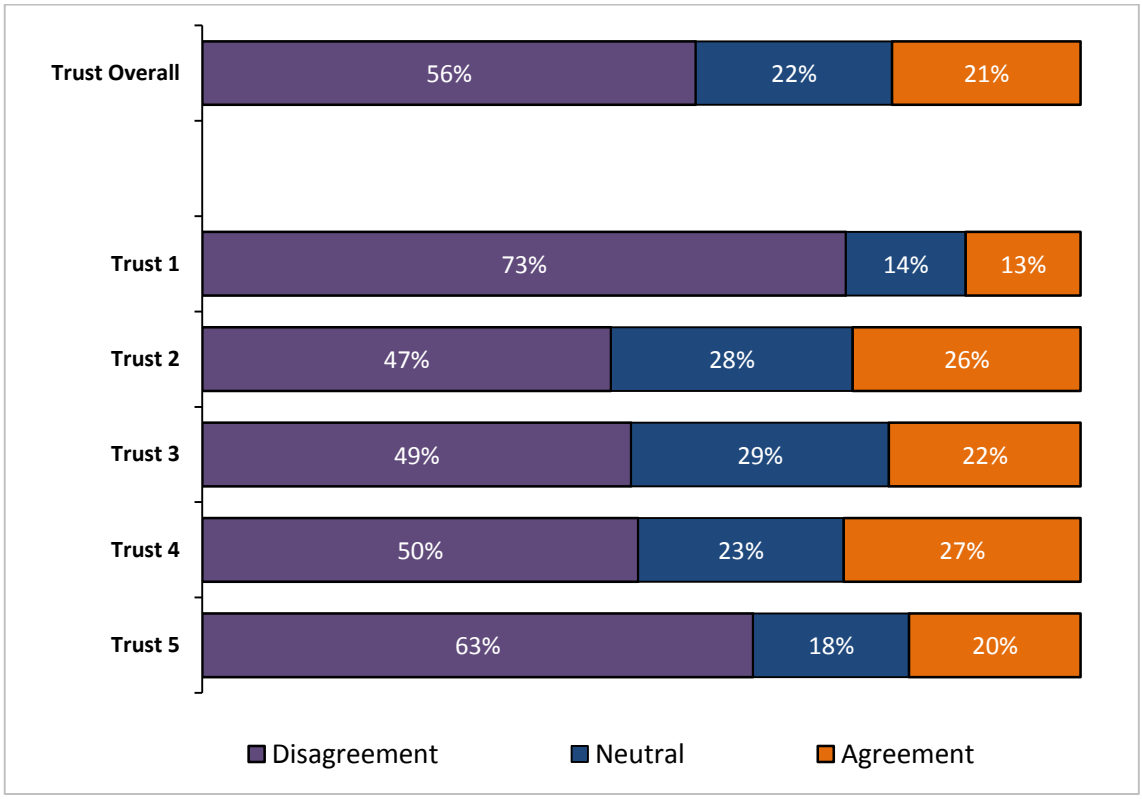

Figure 19: *Trust*

5.5. Results per Privacy Scenario

5.5.1. Privacy Scenario 1

In privacy scenario 1, an incentive was provided to the individual to entice them to disclose personal information (Table 9), however no ability to have the information forgotten (or rather, fully erased), was provided. The results (Figure 20) indicate that, overall, individuals were more likely to disclose personal information and accurate information about themselves (**SCONE 1**) and somewhat likely to disclose work related information (**SCONE 2**).

Table 9: *Privacy scenario 1 questions*

	Question
SCONE 1	Your ability to control who can view your information
SCONE 2	Provide work related information (where you work, project information and your achievements)
SCONE 3	Provide personal information about your friends and family
SCONE 4	Provide financial information (annual income, current debt amount or your cheque account balance)

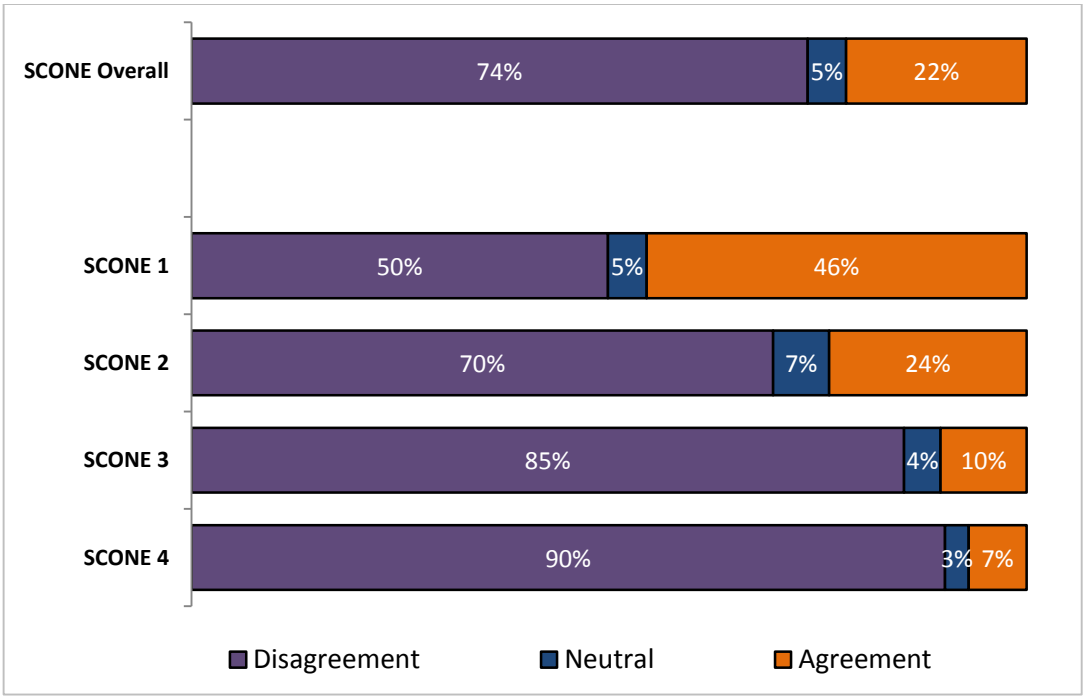

Figure 20: *Privacy scenario 1 responses*

5.5.2. Privacy Scenario 2

In privacy scenario 2, no incentives were given to the individual, however, the ability to have their information forgotten or rather fully erased was provided (Table 10). The results (Figure 21) indicated that, overall, individuals were more inclined (10% more than in privacy scenario 1) to disclose personal information and accurate information about themselves (**SCONE 1**) and somewhat more likely (10% more than in privacy scenario 1) to disclose work related information (**SCONE 2**). Even though they showed more willingness in disclosing personal information regarding friends and family members (**SCONE 3**) and their personal finance (**SCONE 4**), the degree of this disclosure was minimal.

Table 10: *Privacy scenario 2 questions*

	Question
SCTWO 1	Your ability to control who can view your information
SCTWO 2	Provide work related information (where you work, project information and your achievements)
SCTWO 3	Provide personal information about your friends and family
SCTWO 4	Provide financial information (annual income, current debt amount or your cheque account balance)

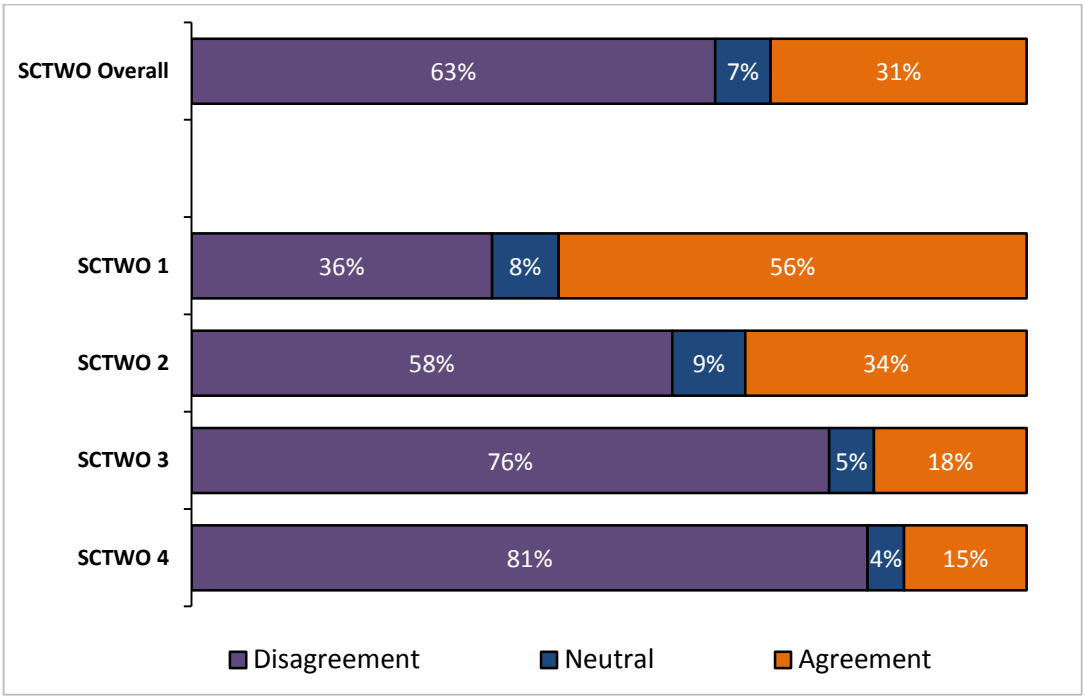

Figure 21: *Privacy scenario 2 responses*

5.5.3. Privacy Scenario 3

In privacy scenario 3, both an incentive and the ability to have their information forgotten or rather fully erased were provided (Table 11). The results (Figure 22) did not considerably differ from those obtained with privacy scenario 1.

Table 11: *Privacy scenario 3 questions*

	Question
SCTHREE 1	Your ability to control who can view your information
SCTHREE 2	Provide work related information (where you work, project information and your achievements)
SCTHREE 3	Provide personal information about your friends and family
SCTHREE 4	Provide financial information (annual income, current debt amount or your cheque account balance)

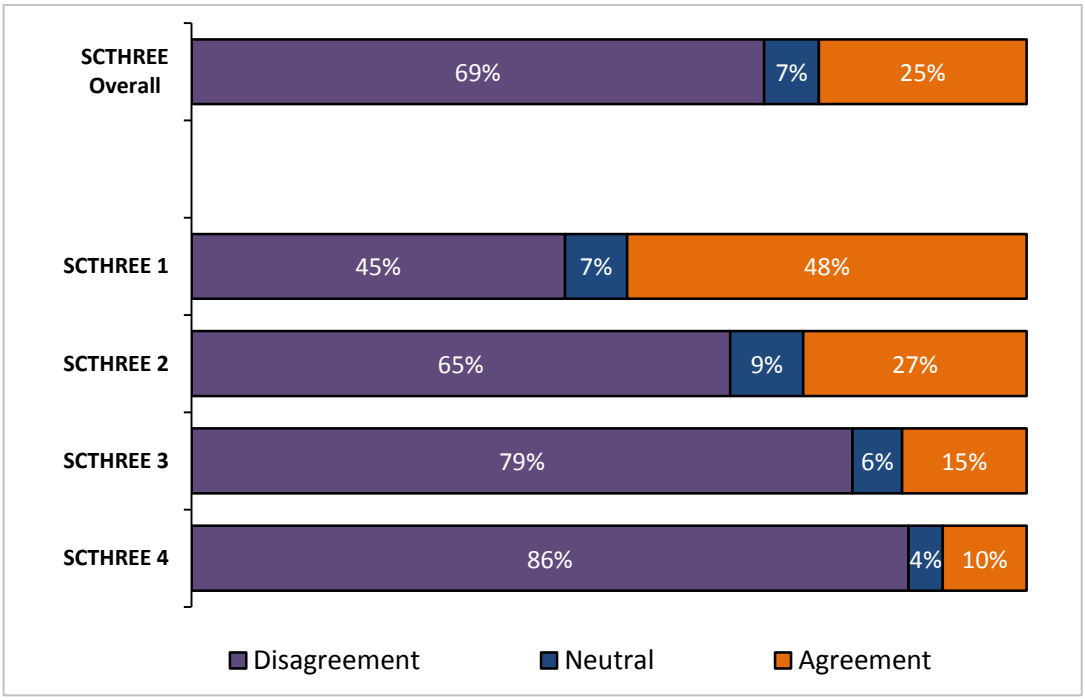

Figure 22: *Privacy scenario 3 responses*

5.6. Results on Reliability and Validity of the Data

The Cronbach's Alpha was used to assess the reliability and validity of the survey and the data. A Composite Construct Reliability (CCR) score and an Average Variance Explained (AVE) score were used to determine the reliability and validity of the constructs during a factor analysis. Additionally, as part of determining construct validity the following types of statistical analyses were performed:

- The Kaiser-Meyer-Olkin (KMO) was used to determine the sample adequacy and sphericity of the item-correlation matrix;
- Exploratory factor analysis was used to discover and identify the dimensions of the measurements.

In the initial pilot, a category called Risk vs Benefits encompassed the questions in Table 12. Questionnaire statements RVB3_REVERSE and RVB4_REVERSE (Table 12) were found to have very low item-total correlations relative to the other statements. When the variable RVB3_REVERSE was deleted, the Cronbach's Alpha result increased from 0.794 to 0.815. Similarly, when the variable RVB4_REVERSE was deleted, the Cronbach's Alpha result increased from 0.794 to 0.804. As a result, these two variables were removed from the Risk vs Benefits scale.

Further factor analysis on the remaining seven statements revealed the presence of two underlying constructs, which had high loadings when separated. Table 13 illustrates the survey statements that loaded highly on these two underlying constructs, which were consequently named Perceived Benefits and Trust. These results for all other constructs and privacy scenarios can be found in Table 16.

Table 12: *Cronbach's Alpha for risk vs benefit scale*

Questionnaire Statements (VARIABLES)	Cronbach Alpha	Mean	Std. Deviation	Corrected Item-Total Correlation	Cronbach Alpha If Item Deleted
The website provides me with the convenience to instantly access the information I need **(RVB1)**	**0.794**	3.357	0.946	0.473	0.776
Overall, I feel that using the website is beneficial **(RVB2)**		3.285	1.004	0.514	0.770
Overall, I see no real threat to my privacy by disclosing personal information to the website **(RVBN1)**		2.111	1.038	0.609	0.757
I think my benefits gained from using the website can offset the risks of my information disclosure **(RVB5)**		2.679	1.132	0.569	0.761
The value I gain from using the website is worth the information I give away **(RVB6)**		2.545	1.073	0.646	0.751
The ability to request that my personal information be destroyed gives me trust in the website **(RVBN2)**		2.627	1.219	0.588	0.758
I would disclose additional personal information to the website because I can request for my information to be destroyed **(RVBN3)**		2.293	1.196	0.576	0.760
I am aware that providing the website with my personal information may involve experiencing unexpected problems **(RVB3_REVERSE)**		2.049	0.888	0.112	0.815
It would be risky to disclose my personal information to the website **(RVB4_REVERSE)**		1.905	0.952	0.229	0.804
Valid N (listwise)	**389**				

Table 13: *Identified new constructs with high loadings*

Questionnaire Statements (VARIABLES)	Construct	Loading
The website provides me with the convenience to instantly access the information I need **(RVB1)**	Perceived Benefits	0.893
Overall, I feel that using the website is beneficial **(RVB2)**		0.911
Overall, I see no real threat to my privacy by disclosing personal information to the website **(RVBN1)**	Trust	0.664
I think my benefits gained from using the website can offset the risks of my information disclosure **(RVB5)**		0.624
The value I gain from using the website is worth the information I give away **(RVB6)**		0.661
The ability to request that my personal information be destroyed gives me trust in the website **(RVBN2)**		0.838
I would disclose additional personal information to the website because I can request for my information to be destroyed **(RVBN3)**		0.844
Valid N (listwise)	**389**	

Table 14 below summarises the factor analysis results for all the constructs. The consistently high KMO statistics and the significant Bartlett's Chi-Squared results indicate that the data was valid to run a factor analysis.

Table 14: *Factor analysis results per privacy calculus construct and privacy scenario*

Construct	KMO	Bartlett's Chi-Squared (df)	Significance (p-value)
Privacy Concern	0.929	2523.008 (28)	<0.001
Need for Awareness	0.760	762.247 (10)	<0.001
Lack of Perceived Control	0.820	1404.071 (15)	<0.001
Perceived Benefits	0.500	361.397 (1)	<0.001
Trust	0.747	810.292 (10)	<0.001
Privacy Scenarios			
Privacy scenario 1 (PS1)	0.742	580.416 (6)	<0.001
Privacy scenario 2 (PS2)	0.759	751.644 (6)	<0.001
Privacy scenario 3 (PS3)	0.744	746.414 (6)	<0.001

The table below illustrates that all variables loaded significantly on the corresponding factors demonstrating construct validity.

Table 15: *Construct validity*

Construct	No of Items	Eigenvalues	Explained Variation (%)
Privacy Concern	8	5.705	71.31
Need for Awareness	5	2.774	55.48
Lack of Perceived Control	6	3.764	62.74
Perceived Benefits	2	1.779	88.97
Trust	5	2.949	58.98
Privacy Scenarios			
Privacy scenario 1 (PS1)	4	2.585	64.63
Privacy scenario 2 (PS2)	4	2.765	69.12
Privacy scenario 3 (PS3)	4	2.753	68.82

The results of the factor analysis highlighted the construct validity of the measurement scales for further statistical data analysis. The reliability and validity results are further confirmed in the table below:

Table 16: *Cronbach's Alpha, CCR and AVE for reliability and validity checking*

Construct	Cronbach's Alpha	CCR	AVE	Square Root of AVE	No. of Items
Privacy Concern	0.942	0.952	0.713	0.844	8
Need for Awareness	0.731	0.855	0.555	0.745	5
Lack of Perceived Control	0.879	0.909	0.627	0.792	6
Perceived Benefits	0.875	0.942	0.890	0.943	2
Trust	0.825	0.878	0.590	0.768	5
Privacy Scenarios					
Privacy scenario 1 (PS1)	0.805	0.879	0.646	0.804	4
Privacy scenario 2 (PS2)	0.847	0.899	0.691	0.831	4
Privacy scenario 3 (PS3)	0.842	0.898	0.688	0.823	4

The results demonstrate excellent reliability and validity as the statistical findings were above the relevant thresholds indicated below:

- Cronbach's Alpha > 0.6 is acceptable
- CCR > 0.7 is an indication of construct reliability
- AVE > 0.5 are treated as indications of construct validity

5.7. Hypothesis Testing

5.7.1. Research Question 1 (RQ1)

The first research question and hypothesis (H1) was to determine if the presence of the RTBF principle influenced individuals when engaging in the privacy calculus. A correlation analysis was used to assess the strength of relationships between pairs of variables i.e. between the constructs and the privacy scenarios. In assessing the relationship between variables, the below benchmarks were used to establish the strength of relationships (M. N. K. Saunders & Bezzina, 2015). The following ranges for the coefficient of correlation were used:

- Range one: -1.0 to -0.7 strong negative relationships
- Range two: -0.7 to -0.3 weak negative relationships
- Range three: -0.3 to +0.3 little or no relationship
- Range four: +0.3 to +0.7 weak positive relationships
- Range five: +0.7 to +1.0 strong positive relationships

The table below presents the correlation results:

Table 17: *Summary of hypothesis 1 results*

Privacy Scenario	Construct	p-value	Spearman correlation	Decision
Privacy scenario 1 (PS1)	Need for Awareness	**0.001****	-0.162	Little negative relationship
	Privacy Concern	**0.006****	-0.137	Little negative relationship
	Lack of Perceived Control	0.296	0.053	No relationship
	Perceived Benefits	**0.000****	0.407	Positive relationship
	Trust	**0.000****	0.409	Positive relationship
Privacy scenario 2 (PS2)	Need for Awareness	**0.002****	-0.155	Little negative relationship
	Privacy Concern	0.059	-0.096	No relationship
	Lack of Perceived Control	0.330	0.049	No relationship
	Perceived Benefits	**0.000****	0.388	Positive relationship
	Trust	**0.000****	0.503	Positive relationship
Privacy scenario 3 (PS3)	Need for Awareness	**0.000****	-0.170	Little negative relationship
	Privacy Concern	**0.048***	-0.100	Little negative relationship
	Lack of Perceived Control	0.816	0.011	No relationship
	Perceived Benefits	**0.000****	0.399	Positive relationship
	Trust	**0.000****	0.463	Positive relationship

** Significance at the 0.01 level (2-tailed).
* Significance at the 0.05 level (2-tailed).

Privacy concern was significantly influenced in the presence of an incentive in both **PS1** and **PS3**. The need for awareness, perceived benefits and trust were significant in all privacy scenarios. The privacy scenario, which only had the RTBF and no incentive (**PS2**) demonstrated the highest correlation regarding trust and had no relationship to privacy concern.

5.7.2. Research Question 2 (RQ2)

The above results indicate that the presence of RTBF principle does influence aspects of the privacy calculus. Individuals engage in the privacy calculus when deciding to disclose information, thus the secondary research hypothesis (H2) investigated if online information disclosure was impacted in the presence of the RTBF principle.

The results for testing H2 are presented in two steps:

- Step 1: Kruskal Wallis results for the three scenarios
- Step 2: Mann-Whitney U results and corresponding charts

Kruskal Wallis analysis of variance was performed to determine which of the individual variables i.e. the three privacy scenarios separately, are significantly different. The Kruskal Wallis results (Table 18) indicated that privacy scenario 1 had no significant difference whereas the other two privacy scenarios had statistically significant differences at the 95% significance level. This illustrated that the RTBF principle had an impact on an individual's level of online information disclosure.

Step 1: Kruskal Wallis results for the three scenarios

Table 18: *Kruskal Wallis results for hypothesis 2 (H2)*

		df	Mean Rank	Chi-Square	Sig.
Privacy scenario 1 (PS1)	Low Information Disclosure (n = 82)	2	180.09	4.649	0.098
	Medium Information Disclosure (n = 209)		191.70		
	High Information Disclosure (n = 98)		214.51		
Privacy scenario 2 (PS2)	Low Information Disclosure (n = 82)	2	161.57	15.496	**0.000***
	Medium Information Disclosure (n = 209)		193.05		
	High Information Disclosure (n = 98)		227.14		
Privacy scenario 3	Low Information Disclosure (n = 82)	2	168.48	10.333	**0.006***
	Medium Information Disclosure (n = 209)		192.89		
	High Information Disclosure (n = 98)		221.70		

Step 2: Mann-Whitney U results and corresponding charts

The Kruskal Wallis test was able to establish a significant difference between the privacy scenarios, however, it cannot determine if there is a significant difference within the sub-categories (low, medium and high). The above results indicated that the presence of the RTBF principle has an impact on information disclosure. To determine the difference in impact of the RTBF principle on individuals with low, medium and high degrees of information disclosure, Mann-Whitney's U test was performed. This test was able to determine how individuals of low, medium and high information disclosure were influenced by the three privacy scenarios.

Figure 23 Figure 23A illustrates the significant difference (Table 19) between individuals who have a low degree of information disclosure and those with a higher degree of information disclosure given the provision of an incentive (Privacy scenario 1). In privacy scenario 2, there were significant differences between all sub-categories. When compared to privacy scenario 1, it was apparent that the magnitude of the gap had increased in privacy scenario 2. Figure 23C illustrates how RTBF combined with an incentive influenced individuals with a high propensity to disclose personal information. A similar pattern was observed in privacy scenario 3 (Figure 23C) whereby there was a significant difference observed between individuals with low and medium degrees of information disclosure compared to those with high degrees of information disclosure (Table 19 – privacy scenario 3) in the presence of the RTBF principle and an incentive. No significant difference was observed between low and medium degrees of information disclosure. Collectively these results indicate that the presence of the RTBF principle does influence information disclosure for individuals that fall within the medium and high degrees of information disclosure categories.

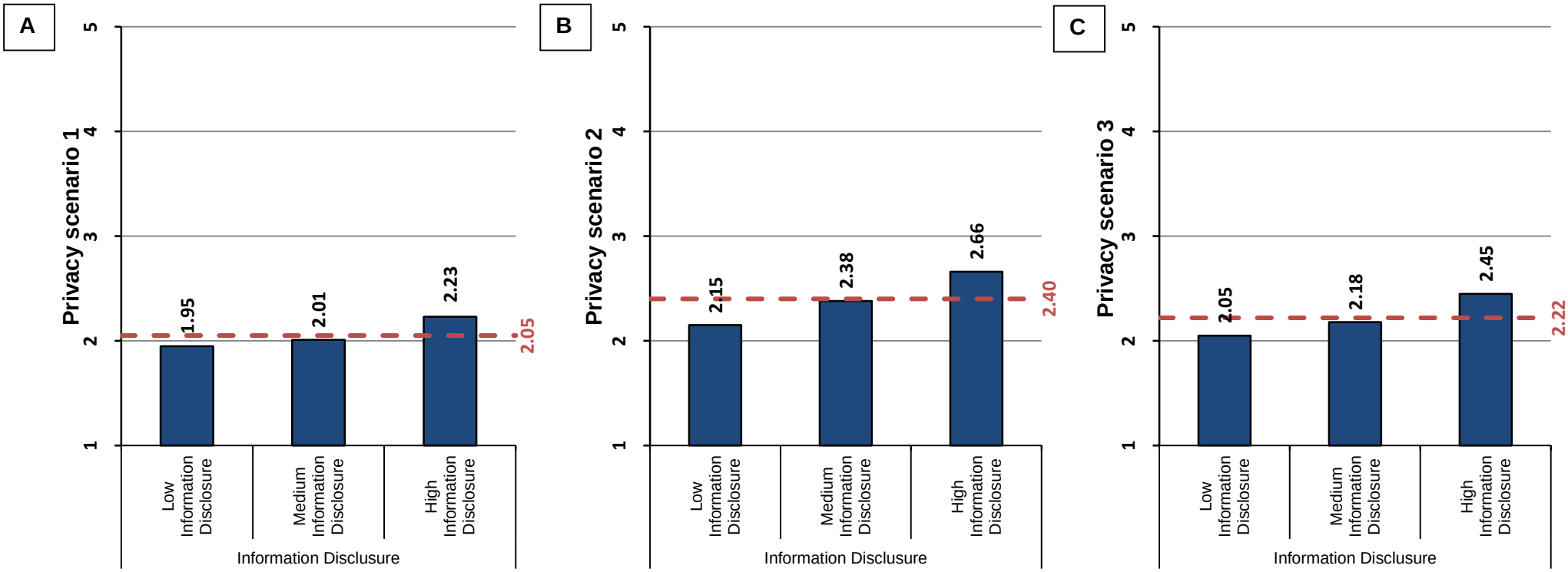

Figure 23: *Average of information disclosure per category of individual.*
Graphical representation of individuals with a low, medium and high degree of information disclosure and their willingness to disclose personal information in the three privacy scenarios. The y-axis represents the scale of how likely an individual is to provide information ranging from 1 = Very unlikely to 5 = Very likely. The number above the boxes indicates the average of respondents in that category whereas the red line represents the average of all respondents in the survey.
Source: Researcher's own construction.

Table 19: *Summary of hypothesis 2 Mann-Whitney U test results*

Privacy Scenario	Construct	U Statistic	p-value	Decision
Privacy scenario 1 (PS1)	Low Information Disclosure against Medium Information Disclosure	8023	0.393	No significance
	Low Information Disclosure against High Information Disclosure	3341.5	**0.050***	Significant difference
	Medium Information Disclosure against High Information Disclosure	9005.5	0.086	No significance
Privacy scenario 2 (PS2)	Low Information Disclosure against Medium Information Disclosure	7142.5	**0.026***	Significant difference
	Low Information Disclosure against High Information Disclosure	2703	**0.000****	Significant difference
	Medium Information Disclosure against High Information Disclosure	8406	**0.011***	Significant difference
Privacy scenario 3 (PS3)	Low Information Disclosure against Medium Information Disclosure	7429.5	0.075	No significance
	Low Information Disclosure against High Information Disclosure	2983	**0.003****	Significant difference
	Medium Information Disclosure against High Information Disclosure	8659.5	**0.028***	Significant difference

** Significance at the 0.01 level (2-tailed).
* Significance at the 0.05 level (2-tailed).

5.8. Conclusion

This chapter aimed to present the results obtained from the survey in an attempt to answer the research questions of the study. Factorial analysis of the constructs within the survey indicated that the results were reliable and valid. All the constructs investigated had high Cronbach alpha values. A Spearman's correlation test was employed to address the first research question, which investigated if the RTBF principle influenced the privacy calculus. It was found that in the presence of the RTBF principle, the need for awareness, perceived benefits and trust components of the privacy calculus were significantly impacted.

Following from this, the second research question, which investigated if the RTBF principle would influence an individual's information disclosure patterns, were answered using various statistical analyses. These tests highlighted that the presence of the RTBF principle does impact information disclosure but is dependent on an individual's degree of online information disclosure. The subsequent chapter will address the meaning of these results in context of what is currently known in literature.

6. CHAPTER 6: DISCUSSION OF RESULTS

6.1. Introduction

The preceding chapter provided the statistical findings of the research instrument outlined in Chapter 4. Chapter 5 presented the results obtained from the self-administered electronic survey after having checked for reliability and validity using Cronbach's Alpha. The statistical tests conducted in this study included Factor Analysis, Spearman's Correlation, Kruskal-Wallis one-way analysis of variance and Mann-Whitney U test.

The RTBF principle (outlined in Section 2.5) is a complex new privacy dimension, which seeks to provide individuals with more control over their personal information when online. Whilst literature on the RTBF have largely focused on its impact on lawmakers and its applicability in maintaining societal interest in the form of freedom of speech and censorship (Ambrose, 2012; Ambrose & Ausloos, 2013; Ausloos, 2012; Bunn, 2015; Corbett, 2013), none could be found which focused on the mental calculation individuals engage in prior to disclosing information online known as the privacy calculus. Furthermore, the effect of the RTBF to an individual's information disclosure pattern remains a largely unanswered question in literature.

This chapter provides interpretations of the results in Chapter 5 substantiated by literature reviewed in Chapter 2. Additionally, the outcome of each research question and corresponding hypotheses are conclusively stated in a manner to ascertain their validity.

6.2. Research Question 1 (RQ1)

The privacy calculus, based on the works of Culnan and Armstrong (1999) and further extended by Dinev and Hart (2006) and Keith et al. (2013), form the literature base for this study. To this extent, constructs were formulated and classified as factors that discourage and factors that promote information disclosure based on the literature reviewed. To ascertain whether the RTBF influences the privacy calculus, three privacy scenarios related to an individual's willingness to disclose personally identifiable information were tested against the identified constructs.

RQ1 provided enquiry on whether the presence of the RTBF has an influence on individuals when engaging in the privacy calculus. This question was posed to

understand how a novel component such as the RTBF principle influences the mental calculations performed by individuals prior to disclosing information online.

6.2.1. Hypothesis 1

The hypotheses for the first research question were stated as:

> **$H1_0$**: The RTBF principle does not influence individuals when engaging in the privacy calculus theory
>
> **$H1_A$:** The RTBF principle does influence individuals when engaging in the privacy calculus theory

To test the hypothesis, each construct, was tested in relation to the various privacy scenarios to identify its effect on the privacy calculus. The constructs tested were as follows:

- Factors that Discourage Individual Information Disclosure
  - Need for awareness
  - Privacy concern
  - Lack of perceived control
- Factors that Promote Individual Information Disclosure
  - Trust
  - Perceived benefits

Each construct was adapted from previous research (see Section 4.8.2) and tested against three privacy scenarios which included one with an incentive (**PS1**), one with no incentive but with the ability to have one's data full erasable i.e. the RTBF principle (**PS2**) and a final scenario which combined both an incentive and the RTBF principle (**PS3**). Each construct was tested using Spearman's correlation and the results are presented in Table 17.

6.2.1.1. Factors that Discourage Individual Information Disclosure

In terms of factors that discourage information disclosure, the need for awareness was the only construct significantly different ($p < 0.05$) in all three privacy scenarios and was most influenced in **PS3**. Figure 16 shows that the respondents had a consensus regarding companies providing more awareness to how their information is used (**Aware1**). Based on respondent feedback, this study supports the literature finding by Capistrano and Chen (2015) on the positive effects a clear and comprehensible privacy policy has on an individual's privacy calculus (**Aware2**). Similarly, respondents

expressed a need to be more knowledgeable about how their information is used by organisations (**Aware3**), thus seeking a way to remove asymmetric information often experienced online Acquisti et al. (2015). Respondents also indicated an active use of privacy filters to control the audience of their posts on SNS (**Aware5**) indicating that with improved privacy controls now embedded within SNS, individuals have become cognisant of the need to limit the audience of their posts on these platforms. This finding contradicts earlier findings by Gross and Acquisti (2005) regarding individuals hardly making use of privacy preferences, however, the change in behaviour could be attributed to the evolution of SNS over the years. Prevalent in the responses is the privacy paradox (Norberg et al., 2007), despite wanting more awareness regarding how their personal information is used, a large majority indicated not reading privacy policies prior to registering for the site (**Aware4**). This behaviour may be attributed to the lengthy nature of such privacy policies or quite simply indicates trust in the service provider to make use of fair information practices as alluded to by Culnan and Armstrong (1999). Despite being statistically significant, there is however insufficient evidence to conclude that the need for awareness has a substantial impact on any of the privacy scenarios.

Privacy concern was found to be significant in both **PS1** ($p < 0.05$) and **PS3** ($p < 0.05$) albeit having little negative relationship to the scenarios. This indicates that privacy concern within these scenarios have a very small impact on the privacy calculus. A possible logical assumption for this may be related to the fact that in both scenarios an incentive was provided to the user thus minimising privacy concerns owing to the fact that economic gain was obtained for the exchange of consumer information. This behaviour is congruent to the privacy calculus theory which weighs the costs and benefits prior to information disclosure, the findings regarding privacy concern when there is evidence of an incentive motivates the findings of Hui et al. (2006) and (Hann, Hui, Lee, & Png, 2007). Given the ability to retract information with the RTBF in **PS2**, there were no relationships with privacy concern. It can be argued that the presence of the RTBF removes privacy concerns as more control is provided to the individual regarding their data thus supporting Young and Quan-Haase (2013) findings on increased control minimizes an individual's anxiety level (concern).

The lack of perceived control had no significance in any of the privacy scenarios.

6.2.1.2. Factors that Promote Individual Information Disclosure

Factors that promote information disclosure namely, perceived benefits and trust were significant in all three privacy scenarios with correlation values higher than the other constructs. In privacy scenarios **PS2** and **PS3**, perceived benefits and trust had strong correlations (Table 17). However, higher correlations were observed regarding trust in **PS2**. The research results support findings by S.-W. Lin and Liu (2012) who found that trust mitigates user privacy concerns in their study. They further emphasis that in order to enhance online service offerings, the dominate factor to focus on is trust.

Trust is an important aspect that needs to be addressed to resolve privacy concerns which, continue to be comprehensively debated in literature (Fogel & Nehmad, 2009; S.-W. Lin & Liu, 2012; Mohamed & Ahmad, 2012). A study by Min and Kim (2015) indicated that 62% of respondents in a survey of over 2300 respondents expressed concern regarding their online security, a finding which corroborates Cho, Rivera-Sánchez, and Lim (2009) who found similar patterns in a multinational study on online privacy.

6.2.1.3. Conclusion for Hypothesis 1

Our findings indicate that the positive relationships in perceived benefits and trust, factors that we categorise as those which promote information disclosure, outweigh those that discourage information disclosure. These same results can be found for **PS2** and **PS3** that both included the presence of the RTBF principle. Given these results, there is sufficient evidence to **reject the null hypothesis** and conclude that the RTBF principle does influence individuals when engaging in the privacy calculus theory. In particular perceived benefits, and trust influence this calculus the most in these scenarios.

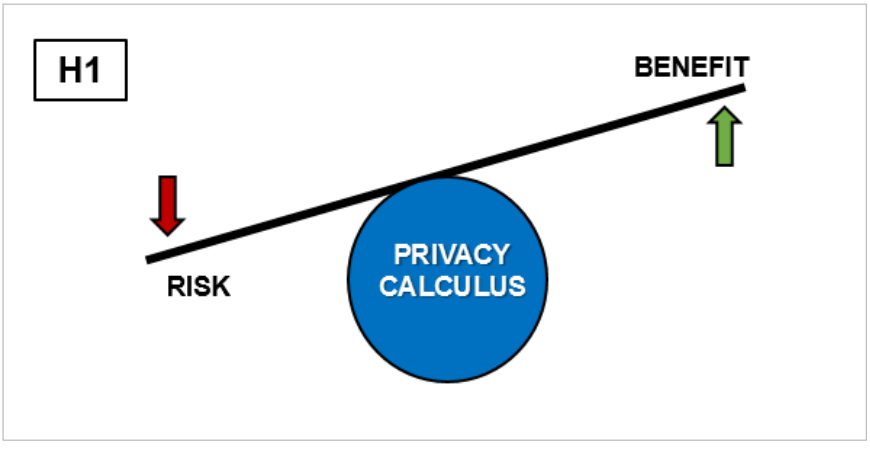

Figure 24: *The RTBF's impact on privacy calculus for hypothesis 1 (H1). The results found sufficient evidence to reject the null hypothesis and conclude that the RTBF principle does influence individuals when engaging in the privacy calculus theory.*
Source: Researcher's own construction.

It can thus be argued that online service providers who integrate the RTBF principle are likely to increase both trust and perceived benefits as a result of providing individuals with more control over their personal information. This also provides organisations with the ability to mitigate consumer concerns about losing control over the way their data is used and disseminated after they've been provided to the organisation as per Wu et al. (2012). This would honour the social contract with the individual (Martin, 2015) and provide the adequate awareness which they desire as indicated in Figure 16.

6.3. Research Question 2 (RQ2)

Within the context of this study, the privacy calculus theory determines the extent of information disclosed by individuals. The previous research hypothesis has illustrated that perceived benefits and trust are impacted in the presence of the RTBF, thus one can presume that individuals may view the RTBF principle as a benefit when engaging in the privacy calculus as evident in **PS2** and **PS3**. Based on this premise, an individual's information disclosure may be influenced by the RTBF principle; hence, the following research question was conceived:

RQ2: Does the RTBF impact individual online information disclosure?

The abundance of personally identifiable information collected on the Internet is growing at an alarming rate and users are becoming increasingly concerned with who has access to their data (Young & Quan-Haase, 2013). This has resulted in hesitation to provide accurate information when online. The survey results show that despite heightened concerns (Figure 15) individuals show attributes that include excessive usage of the Internet (Figure 11) and increased degree of information disclosure (Figure 14) thus highlighting the presence of the privacy paradox within our findings.

6.3.1. Hypothesis 2

The hypotheses for the second research question were stated as:

$H2_0$: The RTBF principle has no impact on individuals when disclosing online information.

$H2_A$: The RTBF principle has an impact on individuals when disclosing online information.

6.3.1.1. Findings for Hypothesis 2

The Spearman's Correlation test illustrated that the RTBF does influence individuals when engaging in the privacy calculus. According to the privacy calculus theory, an increase in benefit would lead to increased information disclosure (Figure 2). Whilst the findings for hypothesis 2 could have been inferred from H1 or the Kruskal Wallis results in Table 18 by looking at the results for **PS2** and **PS3**, this study further investigated the category of individuals likely to be more affected by the RTBF.

Figure 23 shows the mean for each of the three categories of individual information disclosure. Evident in all three scenarios (**PS1**, **PS2** and **PS3**), individuals with a high degree of information disclosure will continue to exhibit the same high disclosure behaviour. This is also proven by the results of the Mann-Whitney U test presented in Table 19 ($p = 0.000$ and $p = 0.006$ for **PS1** and **PS2** respectively) thus confirming findings by Taddei and Contena (2013, p. 267) who stated that "users who are generally willing to disclose a lot of personal information disclose the most on the Social Web". Medium information disclosure individuals exhibited similar behaviours as high disclosure individuals.

Individuals with low information disclosure exhibited the very conservative behaviours towards the willingness to disclose information in **PS1** and **PS3**, thus indicating that they would not be deterred by the impact of an incentive or the combination of an incentive and the RTBF. The research findings supports Taddei and Contena (2013, p. 822) who state that "people who perceive higher threats to privacy are less disposed to disclosing information about the self because they perceive themselves as less able to control information and protect themselves too", which may be the case with individuals with low information disclosure tendencies. The presence of only the RTBF principle in **PS2** impacted all individual disclosure categories although only slightly for low information disclosure individuals ($p = 0.026$).

6.3.2. Conclusion for Hypothesis 2

Our findings have shown that individuals with a medium and high degree of information disclosure are likely to disclose more information in the presence of the RTBF principle.

Therefore, these results provide sufficient evidence to **reject the null hypothesis** and conclude that the RTBF principle has an impact on individuals when disclosing online information. These results allude to the fact that the RTBF principle helps in minimizing the privacy concern due to increased control as was found by Olivero and Lunt (2004).

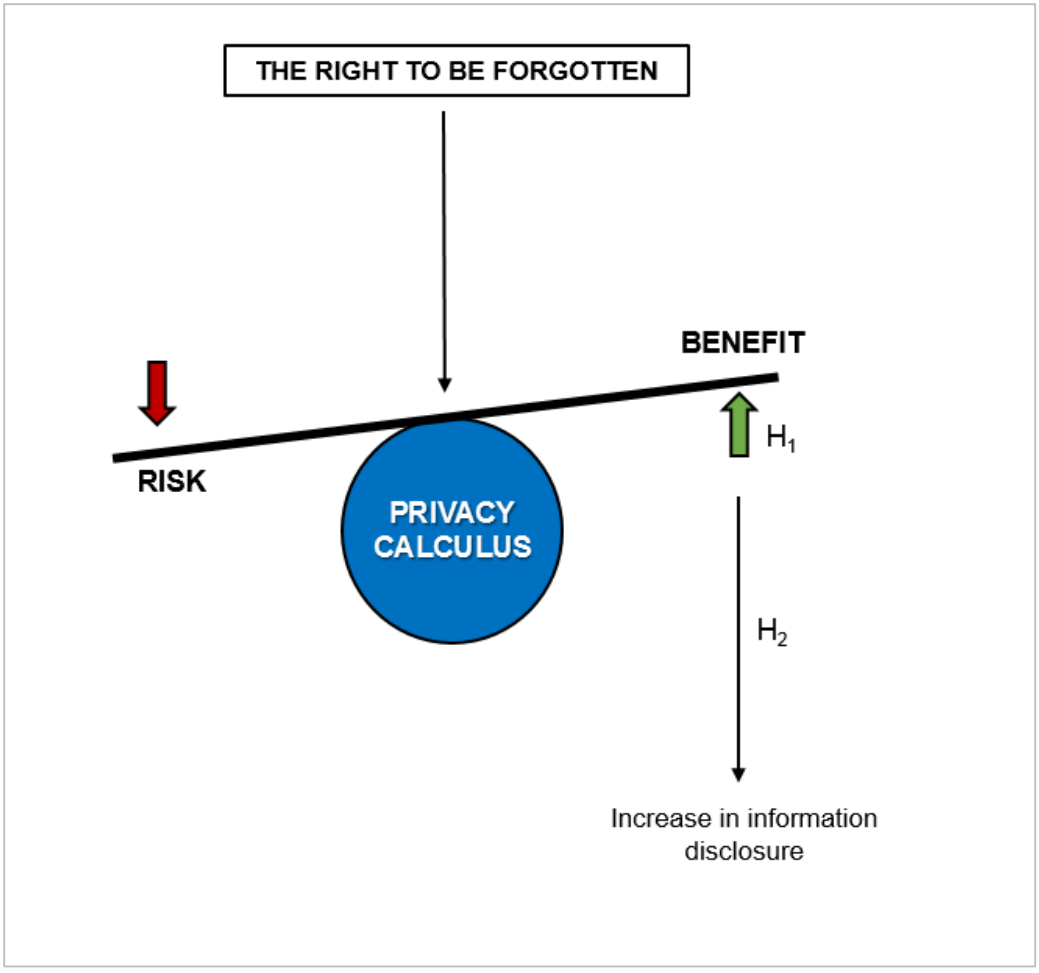

Figure 25: *The RTBF's impact on information disclosure for hypothesis 2 (H2). The results found sufficient evidence to reject the null hypothesis and conclude that the RTBF has an impact on individuals when disclosing online information.*
Source: Researcher's own construction.

6.4. Conclusion

Given the literature reviewed, it appears that the RTBF principle is perceived as a control mechanism, which increases trust and perceived benefits to individuals when engaged in the privacy calculus and evidently increases information disclosure. The findings for the research hypotheses confirm literature covered within Chapter 2.

This study was conducted within the field of social networking and has conclusively shown that given the correct mechanisms of control like the RTBF, individual privacy concerns can be pacified as was found by H. Xu et al. (2011). Additionally, not only does the RTBF principle provide more control to individuals, it also corroborates findings related to an increased level of information disclosure when perceived control is increased (Min & Kim, 2014; Stutzman et al., 2011). If an individual has a higher level of perceived control, it provides a sense of comfort regarding the management of their information, thereby increasing their level of trust and as a result, increasing information disclosure (Joinson et al., 2010; Taddei & Contena, 2013).

Table 20: *Summary of Hypothesis Results*

Hypothesis (null)	**Decision**
$H1_0$: The RTBF principle does not influence individuals when engaging in the privacy calculus theory	Rejected
$H2_0$: The RTBF principle has no impact on individuals when disclosing online information.	Rejected

This chapter provided interpretations of the results presented in Chapter 5. The next chapter concludes the research by providing key highlights of the research, recommendations based on the findings detailed in this chapter. The limitations encountered are also discussed before providing ideas for future research.

7. CHAPTER 7: CONCLUSION

7.1. Introduction

The previous chapter provided interpretation of the results of the research. This concluding chapter highlights the key findings of the research with reference to the primary and secondary objectives of the study, suggests recommendations flowing from the research, proposes further areas of research emanating from this study, and indicates some limitations of this study.

7.2. Main Findings

The research objective of this study was to establish whether the RTBF influences the privacy calculus of individuals when disclosing information online. A secondary objective flowing from the primary objective was to assess whether the RTBF has an impact on information disclosure amongst individuals.

The main findings of this study indicate that the introduction of the RTBF has presented new factors that influence the privacy calculus of individuals. The results outlined in Chapter 5 and interpreted in Chapter 6 indicate that the RTBF principle is perceived as a benefit during the privacy calculus process as it provides individuals with more control over the information they disclose online. Not surprisingly, trust stood out as the most significant factor that influences the calculus. Due to its impact on the privacy calculus, the RTBF has been proven to impact the willingness to disclose information online although the study indicates that this is only prevalent in individuals who have a medium and high degree of information disclosure.

Some of the findings in this research could be of significance in the areas of information technology, international and criminal law, psychology, politics and human rights. Additionally, this study could be used to address individual privacy through amendments to privacy policies, implications on case law and changes in software engineering practices.

7.3. Recommendations

According to Aaron Gabisch and R. Milne (2014, p. 21), “data ownership and privacy control have become an important topic for consumers, marketers and policymakers in today’s digital age”. Hence, there is a need for organisations to find new and innovative ways to minimise the privacy concerns of individuals. Whilst many avenues to achieve

this exist, they have proven inefficient in minimise privacy concerns in a digital era plagued with cyber-attacks, information infringements in the form of breaches and syndicated cybercrime. Managers and organisations alike need to find new innovate ways to provide individuals with transparent, easy and comprehensive mechanisms for the management of their personal information. This may include (and is not limited to), providing information regarding where the individual's data resides physically (country), how their data is processed and if syndicated, to who and in which forms.

The use of privacy policies have proved effective when easily worded (Capistrano & Chen, 2015) however the research results still indicate a majority of individuals within the research sample do not read them. This may be owing to multiple factors, including – the data is not innovatively displayed in a manner that makes sense, the privacy policy contains too much detail or contains too little detail. Indeed privacy policies promote trust in a website and as concluded in this study, trust is the most dominate construct in the privacy calculus. Managers and organisations therefore need to focus efforts on how to improve trust in their online offering to balance the privacy calculus scale towards benefits thus consequently increasing the amount of information an individual is willing to disclose.

From an innovation point of view, new ways to represent privacy controls are needed on websites to allow individuals to manage such settings in an easy and transparent manner. It is the opinion of the researcher that both Facebook and Apple are at the forefront in user interface development that clearly depict active privacy settings of an individual. In part, this may be owing to the fact that both companies have a presence within the European Union and are required to incorporate local laws and principles such as the RTBF and the ability to request for all data relating to them be archived and made available for download. Despite these notable efforts, there is still a lack of transparency regarding where an individual's data is located, how it is used, who has visibility on it and an easy way to erase such information.

In the example of the aforementioned companies, location based information of where one last physically logged into that account is provided but this remains an inefficient and rather dated way to represent the path individual data takes to reach their multitude of servers. An overhaul of interfaces that provide individuals with more control over their data is required. Patagonia, through its Footprint Chronicle (Patagonia, 2015) provides an innovative model for displaying in a real-time the ability to track that taken to produce their apparels. Similar mechanisms can be adopted to allow individuals to track their data in a similar way to how Patagonia tracks the

location of their textile mills, factories and farms on a world map that provides an interactive viewing of statistics per category (Figure 26). Representing visually where one's data is located and how it is used could possibly increase the level of trust in an organisation due to increased visibility and control of removing such data in locations the individual deems unacceptable due to a variety of reasons which may include regulatory reasons, preference based on connectivity speed, diverting areas with political turmoil or countries with Internet censorship. Such an interface could provide options of viewing who has access to the data, how the data was obtained, dates as to when the data was obtained and a simple erasure ("RTBF") mechanism to removing this data.

Technologically, this has proven to be possible and due to syndication agreements organisations have with ad-providers, third party sites and affiliates, the technical construction of such a view is possible however; the complexities of such an implementation are beyond the scope of this study.

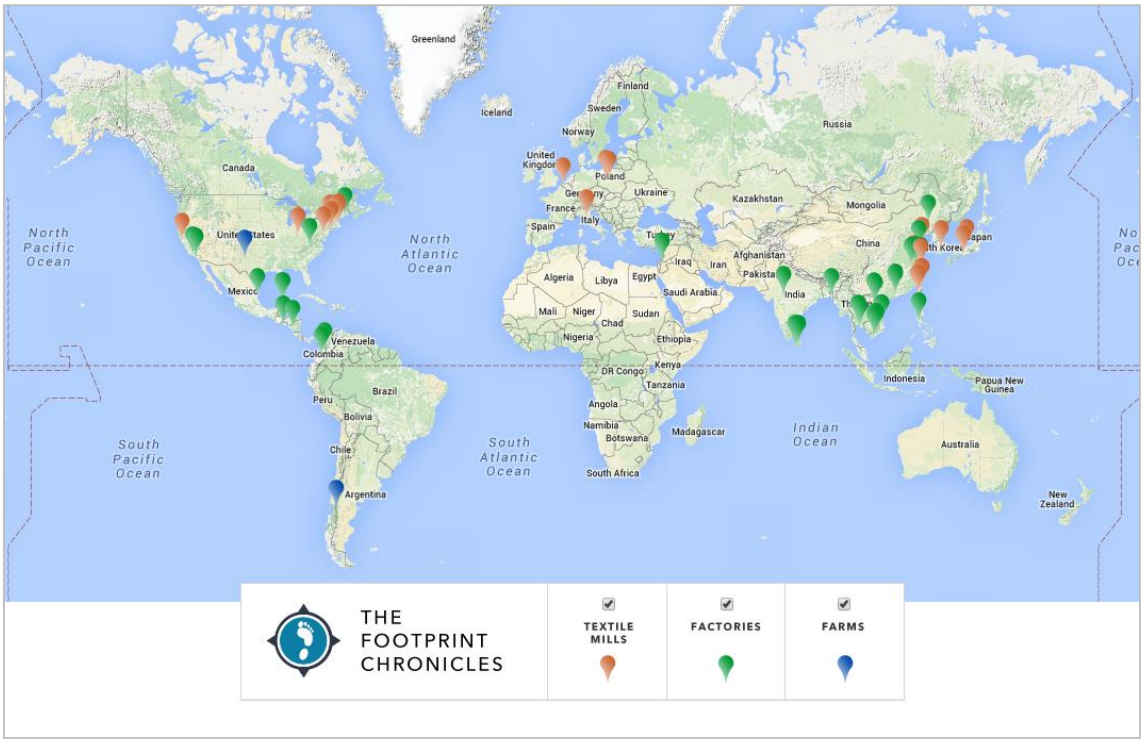

Figure 26: *Proposed transparency model for RTBF.*
World map depicting locations of key elements (shown as pins in red, green and blue) around the world, which could be adapted to present the location of individual data and provide easy erasure policies to enable the RTBF principle.
Source: http://www.patagonia.com/us/footprint

7.4. Ideas for Future Research

A major contention of the RTBF is that it is unknown how this principle will integrate with the civil right of freedom of speech. Studies that can elaborate on the interaction of these two principles is warranted. It would also be beneficial to compare varying organisation's views regarding the impact of the RTBF on the privacy calculus as this study mainly focused on individuals.

The results obtained in this study could only be generalised to the South African population. Future studies could clarify the impact on information disclosure in the presence of the law known as POPI (Protection of Personal Information Bill 2009) which is yet to take effect in South Africa. Under this law, companies may face fines up to R10 million and public announcements of such breaches which would negatively affect the brand image and credibility of such an organisation. Whilst POPI is a reactive consequence of a breach, the context of the RTBF principle remains relevant as subjects can pro-actively request organisations to remove their data prior to a breach. South Africa is classified as part of the BRICS (Brazil, Russia, India, China, and South Africa) countries. Thus, it would be interesting to investigate if the patterns observed in the South African population apply in other BRICS countries and on a global scale.

7.5. Limitations of the Research

While this study serves as a preliminary step towards understanding how the RTBF impacts privacy and information disclosure, it contains certain limitations as discussed in the ensuing paragraphs.

The study focused on investigating if the RTBF principle would have an impact on the privacy calculus and as a result influence information disclosure. The survey only had three privacy scenarios which either included the presence or absence of the RTBF principle in combination with an incentive. However, no scenario was created in which an incentive and the RTBF principle were absent. This information could have been used as an additional control variable as it would have eluded to the baseline responses of individuals regarding their privacy.

The scope of this study was limited to only the "right to erasure" aspect of the RTBF principle. However, the RTBF in its entirety, which would include the "right to be forgotten" and the "right to object", was not investigated. Additionally, the focus of this study was primarily on the impact of the RTBF in the arena of social networking sites

on an individual level. It would be worthy to investigate if the patterns observed in this study transcend to other online platforms such as e-commerce.

Upon completion of the survey it was apparent that majority of the participants were from South Africa whilst only a small proportion were from other countries. The limitations associated with this are two-fold. Firstly, the results of this study cannot be generalised on a global scale. Secondly, the RTBF principle is a relatively novel concept that has primarily drawn attention in Europe. Therefore, South African participants may not have fully understood the intricacies of the RTBF principle.

7.6. Conclusion

This chapter addressed the primary and secondary objectives of the study, regarding the RTBF principle. The data indicated that the majority of respondents were willing to share their personal data, as long as there are some controls in place to guarantee their privacy. Furthermore, some potential uses of the study and further areas of research were recommended. The chapter concludes with some limitations that has to be considered when applying the findings of this study.

8. APPENDICES

8.1. APPENDIX A: Cover Letter

Gordon Institute of Business Science
University of Pretoria

Dear Sir or Madam:

I am conducting my MBA research on how individuals make decisions when disclosing information online and how factors such as the right to be forgotten (which empowers individuals to request that all their personal information be destroyed) impacts this decision process. To that end, you are asked to complete an online survey which should take no longer than 10 minutes in order to provide us with much needed insight for this research.

Your participation is voluntary and you can withdraw at any time without penalty. All data will be kept confidential. By completing the survey, you indicate that you voluntarily participate in this research. If you have any concerns, please contact my supervisor or I, our details are provided below:

Research supervisor details

Supervisor name: Mr Rob Beney

Email address: robbeney@gmail.com

Phone number (mobile): +27 82 333 9853

Researcher details

Researcher name: Nigel Ndaga Mangwanda

Email address: nigel.mangwanda@gmail.com

Phone number (mobile): +27 72 623 4245

8.2. APPENDIX B: Research Survey

SECTION A: Demographics

Thank you for continuing with the survey.

Please complete the below information about yourself.

Note: All answers provided in this survey will be treated as confidential

Please complete the below information about yourself.

Note that all questions in this survey are treated as confidential.

Questions	Answer options
1. How old are you?	Under 24 years old 25 – 34 years old 35 – 45 years old 45 – 55 years old 55 years or older
2. What is your gender?	Male Female Other (please specify)
3. What is the highest degree or level of school you have completed?	No schooling completed Some high school, no diploma High school graduate, diploma or the equivalent Some college credit, no degree Trade/technical/vocational training Bachelors degree Masters degree Doctorate degree
4. In which country do you currently reside?	South Africa Brazil Russia India China Eastern European country Western European country United States of America Australia New Zealand Other
5. What is your ethnicity?	White Black, African or African American Mixed/Multiple ethnic groups Asian/Asian British (Indian, Pakistani, Bangladeshi or Chinese) I would rather not say

SECTION B: Internet Usage Pattern

Please complete the below questions regarding your Internet usage:

Questions	Answer options
6. How long have you been using the Internet?	Less than a year 1 – 3 years 3 – 6 years 7 – 10 years 10 years or more
7. On average, how much time do you spend online each day?	Less than an hour a day 1 – 3 hours a day 3 – 6 hours a day 7 – 10 hours a day 10 or more hours a day
8. Where do you access the Internet most often?	Home computer Work computer Mobile/iPad/Tablet
9. In a typical weekday, do you use the Internet most often for work, for personal reasons, or about an equal amount on both?	A great deal more often for work Quite a bit more often for work Somewhat more often for work About an equal amount for work and personal reasons Somewhat more often for personal reasons Quite a bit more often for personal reasons A great deal more often for personal reasons

SECTION C: Privacy Attitude and Disclosure

On which of the below websites do you have an online profile?

Question 10	Answer options
On which of the below websites do you have an online profile?	Facebook Twittter LinkedIn Piniterest Google+ Tumblr YouTube Instagram Flickr Other (please specify)

Please answer the following questions regarding your online profile(s):

Answer options: Yes or No

Question 11	
11.1	Have you ever created your own profile online that others can see, such as on a social networking site like Facebook, Twitter or LinkedIn?
11.2	Do you allow anyone to view your profile(s)?
11.3	Do you include a picture of yourself on your profile(s)?
11.4	Do you include your e-mail address on your profile(s)?
11.5	Do you include your instant messenger address on your profile(s)?
11.6	Do you include your phone number on your profile(s)?
11.7	Do you include your home address on your profile(s)?
11.8	Do you include information about your interests on your profile(s)?
11.9	Do you include information about your personality on your profile(s)?
11.10	Do you write on other people's profile pages?
11.11	Do you use your real name on your profile page(s)?
11.12	Have you ever created a fake profile(s)?

SECTION D: Privacy Concern

Please indicate your level of agreement with the following statements:

Answer options: 5 Point Likert (Strongly disagree, Disagree, Neither agree or disagree, Agree, Strongly Agree)

Question 12	
12.1	I am concerned that the information I submit on the Internet could be misused
12.2	I am concerned that a person can find personal information about me on the Internet
12.3	I am concerned about submitting information on the Internet because of what others might do with it
12.4	I am concerned about online identity theft
12.5	I am concerned that organisation may keep my information for longer than I anticipate
12.6	I am concerned about submitting information on the Internet because it could be used in a way I did not foresee
12.7	I am concerned that online companies are collecting too much personal information about me
12.8	I am concerned about threats to my personal privacy

SECTION E: Need for Awareness

Please indicate your level of agreement with the following statements:

Answer options: 5 Point Likert (Strongly disagree, Disagree, Neither agree or disagree, Agree, Strongly Agree)

Question 13	
13.1	Companies seeking personal information online should disclose the way the data are collected, processed and used
13.2	A good privacy policy should have a clear and conspicuous disclosure
13.3	It is very important to me that I am aware and knowledgably about how my personal information is used
13.4	I always read the privacy policy before registering for an online service
13.5	I always make use of privacy filters to control who can see certain details on my online profile(s)?

SECTION F: Personal Information Control

How much control do you believe you have over the following issues online (e.g., through policies, privacy settings, etc.). Please indicate your perceived level of control for the following:

Answer options: 5 Point Likert (No control at all, Very little control, I don't know, Sufficient control, Complete control)

Question 14	
14.1	Your ability to control who can view your information?
14.2	Your ability to control the actions of other online users?
14.3	Your ability to correct inaccurate or untruthful information about yourself?
14.4	Your ability to remove embarrassing or damaging information about yourself?
14.5	Your ability to prevent your data and actions from being used/analysed by online companies in ways that you did not intend?
14.6	Your ability to prevent your data and actions from being used/analysed by other parties in ways that you did not intend?

SECTION G: Privacy Scenario 1

SCENARIO 1: You are visiting a website of a discount club. The club offers discounts on consumer products (e.g, electronics, CDs, books) to its members.

Generally, an annual membership fee is R 1000.00 ($90.00 US Dollars). To obtain free membership, you are required to fill out some personal information.

Given this hypothetical scenario, please specify the extent to which you are likely to provide this information through the Internet:

Answer options: 5 Point Likert (Very unlikely, Unlikely, I don't know, Somewhat likely, Very likely)

Question 15	
15.1	Provide accurate personal information about yourself?
15.2	Provide work related information for the purpose of connecting you with colleagues?
15.3	Provide personal information about your friends and family?
15.4	Provide financial information (annual income, current debt amount or your cheque account balance)?

SECTION H: Privacy Scenario 2

SCENARIO 2: You are visiting a website of a discount club. The club offers discounts on consumer products (e.g, electronics, CDs, books) to its members.

In order for the website to present better discount deals to you based on your preferences, you are required to fill out some personal information.

The website provides you with the ability to request that ALL your information be destroyed (from the company and third parties) at any time.

Given this hypothetical scenario, please specify the extent to which you are likely to provide this information through the Internet:

Answer options: Likert (Very unlikely, Unlikely, I don't know, Somewhat likely, Very likely)

Question 16	
16.1	Provide accurate personal information about yourself?
16.2	Provide work related information for the purpose of connecting you with colleagues?
16.3	Provide personal information about your friends and family?
16.4	Provide financial information (annual income, current debt amount or your cheque account balance)?

SECTION I: Privacy Scenario 3

SCENARIO 3: You are visiting a website of a discount club. The club offers discounts on consumer products (e.g, electronics, CDs, books) to its members.

Generally, an annual membership fee is R 1000.00 ($90.00 US Dollars). To obtain free membership, you are required to fill out some personal information.

The website provides you with the ability to request that ALL your information be destroyed (from the company and third parties) any time after your first 3 months of membership.

Given this hypothetical scenario, please specify the extent to which you are likely to provide this information through the Internet:

Answer options: 5 Point Likert (Very unlikely, Unlikely, I don't know, Somewhat likely, Very likely)

Question 17	
17.1	Provide accurate personal information about yourself?
17.2	Provide work related information for the purpose of connecting you with colleagues?
17.3	Provide personal information about your friends and family?
17.4	Provide financial information (annual income, current debt amount or your cheque account balance)?

SECTION J: Risk vs Benefits

Considering your responses on the 3 scenarios (questions 15, 16 and 17), please indicate your level of agreement with the following statements based on your decisions:

Answer options: Likert (Strongly disagree, Disagree, Neither agree or disagree, Agree, Strongly Agree)

Question 18	
18.1	The website provides me with the convenience to instantly access the information I need
18.2	Overall, I feel that using the website is beneficial
18.3	I am aware that providing the website with my personal information may involve experiencing unexpected problems
18.4	It would be risky to disclose my personal information to the website
18.5	Overall, I see no real threat to my privacy by disclosing personal information to the website
18.6	I think my benefits gained from using the website can offset the risks of my information disclosure
18.7	The value I gain from using the website is worth the information I give away
18.8	The ability to request that my personal information be destroyed gives me trust in the website
18.9	I would disclose additional personal information to the website because I can request for my information to be destroyed

8.3. APPENDIX C: Summary Statistics of Pilot Study

Table 21: *Demographic results from the pilot study (n=19)*

Demographics	Category	Frequency	%
Gender	Female	7	36.8
	Male	12	63.2
Age	< 24	3	15.8
	25 – 34	10	52.6
	35 – 45	5	26.3
	45 – 55	1	5.3
Country of residence	South Africa	19	100
Ethnicity	White	7	36.8
	Black, Africa or African American	9	47.4
	Asian/Asian British	2	10.5
	I would rather not say	1	5.3
Internet access location	Home computer	0	0
	Work computer	12	63.2
	Mobile/iPad/Tablet	6	31.6
	Other	1	5.3

Table 22: *Reliability results of pilot study*

Construct	Cronbach's Alpha	Number of Items
Privacy Concern	0.975	8
Need for Awareness	0.778	4
Personal Information Control	0.906	6
Privacy scenario 1	0.861	4
Privacy scenario 2	0.904	4
Privacy scenario 3	0.873	4
Risk vs. Benefits	0.800	6

8.4. APPENDIX D: Summary of Descriptive Statistics

Table 23: *Summary of demographic profile of sample (n=389)*

Demographics	Category	Frequency	%
Gender	Female	200	51.40%
	Male	189	48.60%
	Other	0	0.00%
Age	< 24	210	9.80%
	25 – 34	108	53.00%
	35 – 45	21	28.00%
	45 – 55	77	8.20%
	55 or older	12	1.00%
Country of residence	South Africa	353	90.70%
	Non South African	36	9.30%
Ethnicity	White	189	48.60%
	Black, Africa or African American	91	23.40%
	Mixed/Multiple ethnic groups	20	5.10%
	Asian/Asian British	71	18.30%
	I would rather not say	10	2.60%
	Other ethnic group	8	2.00%
Internet access location	Home computer	50	12.90%
	Work computer	147	37.80%
	Mobile/iPad/Tablet	183	47.00%
	Other	9	2.30%

8.5. APPENDIX E: Central Tendency Statistics per Construct

8.5.1. Privacy Concern

Questionnaire Statements (VARIABLES)	Range	Minimum	Maximum	Interquartile Range	Mean	Std. Deviation	Variance		Skewness
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error
I am concerned that the information I submit on the Internet could be misused **(PC1)**	4	1	5	1	4.062	0.985	0.970	-1.262	0.124
I am concerned that a person can find personal information about me on the Internet **(PC2)**	4	1	5	1	3.936	1.020	1.040	-1.044	0.124
I am concerned about submitting information on the Internet because of what others might do with it **(PC3)**	4	1	5	1	3.936	1.042	1.086	-1.025	0.124
I am concerned about online identity theft **(PC4)**	4	1	5	1	4.075	1.032	1.064	-1.240	0.124
I am concerned that organisations may keep my information for longer than I anticipate **(PC5)**	4	1	5	2	3.869	1.063	1.130	-0.746	0.124
I am concerned about submitting information on the Internet because it could be used in a way I did not foresee **(PC6)**	4	1	5	1	4.018	0.983	0.966	-1.149	0.124
I am concerned that online companies are collecting too much personal information about me **(PC7)**	4	1	5	2	3.913	1.090	1.188	-0.846	0.124
I am concerned about threats to my personal privacy **(PC8)**	4	1	5	2	3.936	1.107	1.225	-0.950	0.124
Privacy Concern (PC_AVE)	**4**	**1**	**5**	**1**	**3.968**	**0.878**	**0.771**	**-1.130**	**0.124**

8.5.2. Need for Awareness

Questionnaire Statements (VARIABLES)	Range	Minimum	Maximum	Interquartile Range	Mean	Std. Deviation	Variance	Skewness	
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error
Companies seeking personal information online should disclose the way the data is collected, processed and used **(AWARE1)**	4	1	5	1	4.476	0.709	0.503	-1.724	0.124
A good privacy policy should have a clear and conspicuous disclosure **(AWARE2)**	4	1	5	1	4.504	0.691	0.477	-1.710	0.124
It is very important to me that I am aware and knowledgeable about how my personal information is used **(AWARE3)**	4	1	5	1	4.494	0.717	0.513	-1.773	0.124
I always read the privacy policy before registering for an online service **(AWARE4)**	4	1	5	2	3.000	1.239	1.536	0.139	0.124
I always make use of privacy filters to control who can see certain details on my online profile(s) **(AWARE5)**	4	1	5	2	3.956	1.070	1.145	-0.953	0.124
Need for Awareness (AWARE_AVE)	**4**	**1**	**5**	**1**	**4.086**	**0.634**	**0.402**	**-1.181**	**0.124**

8.5.3. Lack of Perceived Control

Questionnaire Statements (VARIABLES)	Range	Minimum	Maximum	Interquartile Range	Mean	Std. Deviation	Variance	Skewness	
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error
Your ability to control who can view your information? **(CONTROL1)**	4	1	5	1	3.339	1.039	1.080	-0.535	0.124
Your ability to control the actions of other online users? **(CONTROL2)**	4	1	5	2	2.332	1.122	1.258	0.553	0.124
Your ability to correct inaccurate or untruthful information about yourself? **(CONTROL3)**	4	1	5	2	2.936	1.150	1.323	0.085	0.124
Your ability to remove embarrassing or damaging information about yourself? **(CONTROL4)**	4	1	5	2	2.807	1.182	1.398	0.209	0.124
Your ability to prevent your data and actions from being used/analysed by online companies in ways that you did not intend? **(CONTROL5)**	4	1	5	2	2.324	1.114	1.240	0.618	0.124
Your ability to prevent your data and actions from being used/analysed by other parties in ways that you did not intend? **(CONTROL6)**	4	1	5	2	2.306	1.129	1.275	0.652	0.124
Lack of Perceived Control (CONTROL_AVE)	**4**	**1**	**5**	**1**	**2.674**	**0.888**	**0.788**	**0.467**	**0.124**

8.5.4. Perceived Benefits

Questionnaire Statements (VARIABLES)	Range	Minimum	Maximum	Interquartile Range	Mean	Std. Deviation	Variance	Skewness	
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error
The website provides me with the convenience to instantly access the information I need **(RVB1)**	4	1	5	1	3.357	0.946	0.895	-0.566	0.124
Overall, I feel that using the website is beneficial **(RVB2)**	4	1	5	1	3.285	1.004	1.009	-0.565	0.124
Perceived Benefits (BEN_AVE)	**4**	**1**	**5**	**1**	**3.321**	**0.920**	**0.846**	**-0.590**	**0.124**

8.5.5. Trust

Questionnaire Statements (VARIABLES)	Range	Minimum	Maximum	Interquartile Range	Mean	Std. Deviation	Variance	Skewness	
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error
Overall, I see no real threat to my privacy by disclosing personal information to the website **(RVBN1)**	4	1	5	2	2.111	1.038	1.078	0.861	0.124
I think my benefits gained from using the website can offset the risks of my information disclosure **(RVB5)**	4	1	5	2	2.679	1.132	1.280	0.173	0.124
The value I gain from using the website is worth the information I give away **(RVB6)**	4	1	5	1	2.545	1.073	1.151	0.078	0.124
The ability to request that my personal information be destroyed gives me trust in the website **(RVBN2)**	4	1	5	2	2.627	1.219	1.487	0.255	0.124
I would disclose additional personal information to the website because I can request for my information to be destroyed **(RVBN3)**	4	1	5	2	2.293	1.196	1.429	0.601	0.124
Trust (TRUST_AVE)	**4**	**1**	**5**	**1**	**2.451**	**0.870**	**0.757**	**0.128**	**0.124**

8.5.6. Privacy Scenario 1

Questionnaire Statements (VARIABLES)	Range	Minimum	Maximum	Interquartile Range	Mean	Std. Deviation	Variance	Skewness

	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error
Provide accurate personal information about yourself? **(SCONE1)**	4	1	5	3	2.794	1.394	1.942	0.010	0.124
Provide work related information (where you work, project information and your achievements)? **(SCONE2)**	4	1	5	2	2.213	1.261	1.591	0.746	0.124
Provide personal information about your friends and family? **(SCONE3)**	4	1	5	1	1.728	1.007	1.013	1.497	0.124
Provide financial information (annual income, current debt amount or your cheque account balance)? **(SCONE4)**	4	1	5	1	1.481	0.921	0.848	2.226	0.124
Privacy scenario One (SCONE_AVE)	**4**	**1**	**5**	**1**	**2.054**	**0.922**	**0.850**	**0.817**	**0.124**

8.5.7. Privacy Scenario 2

Questionnaire Statements (VARIABLES)	Range	Minimum	Maximum	Interquartile Range	Mean	Std. Deviation	Variance	Skewness	
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error
Provide accurate personal information about yourself? **(SCTWO1)**	4	1	5	2	3.185	1.319	1.739	-0.385	0.124
Provide work related information (where you work, project information and your achievements)? **(SCTWO2)**	4	1	5	3	2.542	1.351	1.826	0.338	0.124
Provide personal information about your friends and family? **(SCTWO3)**	4	1	5	1	2.046	1.211	1.467	1.057	0.124
Provide financial information (annual income, current debt amount or your cheque account balance)? **(SCTWO4)**	4	1	5	1	1.828	1.179	1.390	1.390	0.124
Privacy scenario Two (SCTWO_AVE)	**4**	**1**	**5**	**1**	**2.400**	**1.049**	**1.100**	**0.642**	**0.124**

8.5.8. Privacy Scenario 3

Questionnaire Statements (VARIABLES)	Range	Minimum	Maximum	Interquartile Range	Mean	Std. Deviation	Variance	Skewness	
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error
Provide accurate personal information about yourself? **(SCTHREE1)**	4	1	5	2	2.931	1.358	1.843	-0.116	0.124
Provide work related information (where you work, project information and your achievements)? **(SCTHREE2)**	4	1	5	3	2.357	1.304	1.699	0.592	0.124
Provide personal information about your friends and family? **(SCTHREE3)**	4	1	5	1	1.920	1.129	1.275	1.173	0.124
Provide financial information (annual income, current debt amount or your cheque account balance)? **(SCTHREE4)**	4	1	5	1	1.676	1.044	1.091	1.702	0.124
Privacy scenario Three (SCTHREE_AVE)	**4**	**1**	**5**	**2**	**2.221**	**1.001**	**1.002**	**0.748**	**0.124**

9. REFERENCES

Aaron Gabisch, J., & R. Milne, G. (2014). The impact of compensation on information ownership and privacy control. *Journal of Consumer Marketing, 31*(1), 13-26.

Acquisti, A. (2010). The economics of personal data and the economics of privacy.

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509-514. doi:10.1126/science.aaa1465

Acquisti, A., & Gross, R. (2006). *Imagined communities: Awareness, information sharing, and privacy on the Facebook.* Paper presented at the Privacy enhancing technologies.

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy*(1), 26-33.

Adkinson, W. F., Eisenach, J. A., & Lenard, T. M. (2002). Privacy online: A report on the information practices and policies of commercial web sites. *Progress and Freedom Foundation, Washington DC*.

Adomavicius, G., & Tuzhilin, A. (2005). Personalization technologies: a process-oriented perspective. *Communications of the ACM, 48*(10), 83-90.

Afroz, S., Islam, A. C., Santell, J., Chapin, A., & Greenstadt, R. (2013, 29-29 June 2013). *How Privacy Flaws Affect Consumer Perception.* Paper presented at the Socio-Technical Aspects in Security and Trust (STAST), 2013 Third Workshop on.

Ahn, Y.-Y., Han, S., Kwak, H., Moon, S., & Jeong, H. (2007). *Analysis of topological characteristics of huge online social networking services.* Paper presented at the Proceedings of the 16th international conference on World Wide Web.

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

Al-Daraiseh, A. A., Al-Joudi, A. S., Al-Gahtani, H. B., & Al-Qahtani, M. S. (2014). Social Networks Benefits, Privacy, and Identity Theft: KSA Case Study. *International Journal of Advanced Computer Science and Applications, 5*(12).

Almeida, V. A. (2012). Privacy Problems in the Online World. *Internet Computing, IEEE, 16*(2), 4-6.

Ambrose, M. L. (2012). It's about time: Privacy, information lifecycles, and the right to be forgotten. *Stanford Technology Law Review, 16*.

Ambrose, M. L. (2014). Speaking of forgetting: Analysis of possible non-EU responses to the right to be forgotten and speech exception. *Telecommunications Policy, 38*(8–9), 800-811. doi:http://dx.doi.org/10.1016/j.telpol.2014.05.002

Ambrose, M. L., & Ausloos, J. (2013). The right to be forgotten across the pond. *Journal of Information Policy, 3*, 1-23.

Ausloos, J. (2012). The 'Right to be Forgotten' – Worth remembering? *Computer Law & Security Review, 28*(2), 143-152. doi:http://dx.doi.org/10.1016/j.clsr.2012.01.006

Awad, N. F., & Krishnan, M. S. (2006). The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization. *Mis Quarterly, 30*(1), 13-28. doi:10.2307/25148715

Baek, Y. M. (2014). Solving the privacy paradox: A counter-argument experimental approach. *Computers in Human Behavior, 38*(0), 33-42. doi:http://dx.doi.org/10.1016/j.chb.2014.05.006

Bansal, G., & Zahedi, F. M. (2015). Trust violation and repair: The information privacy perspective. *Decision Support Systems, 71*, 62-77.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday, 11*(9).

Belk, R. (2014). You are what you can access: Sharing and collaborative consumption online. *Journal of Business Research, 67*(8), 1595-1600.

Bella, G., Giustolisi, R., & Riccobene, S. (2011). Enforcing privacy in e-commerce by balancing anonymity and trust. *Computers & Security, 30*(8), 705-718. doi:http://dx.doi.org/10.1016/j.cose.2011.08.005

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

Bornstein, M. H., Jager, J., & Putnick, D. L. (2013). Sampling in developmental science: Situations, shortcomings, solutions, and standards. *Developmental Review, 33*(4), 357-370.

Botsman, R., & Rogers, R. (2011). *What's mine is yours: How collaborative consumption is changing the way we live*: Collins London.

Boyd, D. M., & Ellison, N. B. (2007). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication, 13*(1), 210-230. doi:10.1111/j.1083-6101.2007.00393.x

Brady, N. (2014). Does the 'right of erasure' pose a bigger threat than the 'right to be forgotten'? Retrieved from http://www.theguardian.com/media-network/media-network-blog/2014/jul/10/right-forgotten-google-data-protection

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2012). Misplaced Confidences: Privacy and the Control Paradox. *Social Psychological and Personality Science, 4*(3), 340-347. doi:10.1177/1948550612455931

Bunn, A. (2015). The curious case of the right to be forgotten. *Computer Law & Security Review, 31*(3), 336-350. doi:http://dx.doi.org/10.1016/j.clsr.2015.03.006

Capistrano, E. P. S., & Chen, J. V. (2015). Information privacy policies: The effects of policy characteristics and online experience. *Computer Standards & Interfaces, 42*, 24-31.

Case, C. J., King, D. L., & Gage, L. M. (2015). Online Privacy and Security at the Fortune 500: An empirical examination of practices. *ASBBS eJournal, 11*(1), 59-67.

Caudill, E. M., & Murphy, P. E. (2000). Consumer online privacy: Legal and ethical issues. *Journal of Public Policy & Marketing, 19*(1), 7-19.

Cetto, A., Netter, M., Pernul, G., Richthammer, C., Riesner, M., Roth, C., & Sänger, J. (2014). *Friend Inspector: A Serious Game to Enhance Privacy Awareness in Social Networks.* Paper presented at the In Proc. of the 2nd International Workshop on Intelligent Digital Games for Empowerment and Inclusion (IDGEI).

Chen, B., & Marcus, J. (2012). Students' self-presentation on Facebook: An examination of personality and self-construal factors. *Computers in Human Behavior, 28*(6), 2091-2099.

Cheung, C., Lee, Z. W. Y., & Chan, T. K. H. (2015). Self-disclosure in social networking sites. *Internet Research, 25*(2), 279-299. doi:10.1108/IntR-09-2013-0192

Cheung, C. M. K., Chiu, P.-Y., & Lee, M. K. O. (2011). Online social networks: Why do students use facebook? *Computers in Human Behavior, 27*(4), 1337-1343. doi:10.1016/j.chb.2010.07.028

Cheung, C. M. K., & Lee, M. K. O. (2006). Understanding consumer trust in Internet shopping: A multidisciplinary approach. *Journal of the American Society for Information Science and Technology, 57*(4), 479-492. doi:10.1002/asi.20312

Chiang, J. K.-H., & Suen, H.-Y. (2015). Self-presentation and hiring recommendations in online communities: Lessons from LinkedIn. *Computers in Human Behavior, 48*, 516-524. doi:http://dx.doi.org/10.1016/j.chb.2015.02.017

Cho, H., Rivera-Sánchez, M., & Lim, S. S. (2009). A multinational study on online privacy: global concerns and local responses. *new media & society, 11*(3), 395-416.

Cohen, R., & Hiller, J. (2002). *Internet law and policy*: Prentice Hall Professional Technical Reference.

Cooper, D. R., & Schindler, P. S. (2013). *Business Research Methods: 12th Edition*: McGraw-Hill Higher Education.

Corbett, S. (2013). The retention of personal information online: A call for international regulation of privacy law. *Computer Law & Security Review, 29*(3), 246-254. doi:http://dx.doi.org/10.1016/j.clsr.2013.03.005

Culnan, M. J. (1993). "How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use. *Mis Quarterly*, 341-363.

Culnan, M. J. (2000). Protecting Privacy Online: Is Self-Regulation Working? *Journal of Public Policy & Marketing, 19*(1), 20-26. doi:10.2307/30000484

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

Cumbley, R., & Church, P. (2013). Is “Big Data” creepy? *Computer Law & Security Review, 29*(5), 601-609. doi:http://dx.doi.org/10.1016/j.clsr.2013.07.007

De Wolf, R., Willaert, K., & Pierson, J. (2014). Managing privacy boundaries together: Exploring individual and group privacy management strategies in Facebook. *Computers in Human Behavior, 35*(0), 444-454. doi:http://dx.doi.org/10.1016/j.chb.2014.03.010

Debatin, B., Lovejoy, J. P., Horn, A.-K., & Hughes, B. N. (2009). Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. *Journal of Computer-Mediated Communication, 15*(1), 83-108. doi:10.1111/j.1083-6101.2009.01494.x

Denscombe, M. (2014). *The good research guide for small-scale social research projects*: McGraw-Hill Education (UK).

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), 285-297. doi:10.1002/ejsp.2049

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

Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance – An empirical investigation. *The Journal of Strategic*

Information Systems, 17(3), 214-233. doi:http://dx.doi.org/10.1016/j.jsis.2007.09.002

Doherty, C., & Lang, M. (2014). *An Exploratory Survey of the Effects of Perceived Control and Perceived Risk on Information Privacy.* Paper presented at the 9th Annual Symposium on Information Assurance (ASIA'14).

Donaldson, T., & Dunfee, T. W. (1994). Toward a unified conception of business ethics: Integrative social contracts theory. *Academy of management review, 19*(2), 252-284.

Eastlick, M. A., Lotz, S. L., & Warrington, P. (2006). Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. *Journal of Business Research, 59*(8), 877-886. doi:10.1016/j.jbusres.2006.02.006

Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The Benefits of Facebook "Friends:" Social Capital and College Students' Use of Online Social Network Sites. *Journal of Computer-Mediated Communication, 12*(4), 1143-1168. doi:10.1111/j.1083-6101.2007.00367.x

Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook "friends:" Social capital and college students' use of online social network sites. *Journal of Computer-Mediated Communication, 12*(4), 1143-1168.

Euromonitor International. (2015). *Internet Users: Euromonitor International from International Telecommunications Union/OECD/national statistics*. Retrieved from http://0-www.portal.euromonitor.com.innopac.up.ac.za/portal/statistics/tab

European Commission. (2014). *European Commission: Fact sheet on the right to be forgotten ruling (C-131/12)*. Retrieved from http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf.

Finn, R. L., & Wright, D. (2012). Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications. *Computer Law & Security Review, 28*(2), 184-194. doi:http://dx.doi.org/10.1016/j.clsr.2012.01.005

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

Fricker, R. D., & Schonlau, M. (2002). Advantages and disadvantages of Internet research surveys: Evidence from the literature. *Field methods, 14*(4), 347-367.

Friedman, B., Khan Jr, P. H., & Howe, D. C. (2000). Trust online. *Communications of the ACM, 43*(12), 34-40.

Frye, N. E., & Dornisch, M. M. (2010). When is trust not enough? The role of perceived privacy of communication tools in comfort with self-disclosure. *Computers in*

Human Behavior, 26(5), 1120-1127. doi:http://dx.doi.org/10.1016/j.chb.2010.03.016

Gefen, D., Rao, V. S., & Tractinsky, N. (2003). *The conceptualization of trust, risk and their electronic commerce: the need for clarifications.* Paper presented at the System Sciences, 2003. Proceedings of the 36th Annual Hawaii International Conference.

Gibbs, S. (2015). French data regulator rejects Google's right-to-be-forgotten appeal Retrieved from http://www.theguardian.com/technology/2015/sep/21/french-google-right-to-be-forgotten-appeal

Gray, D. E. (2013). *Doing research in the real world*: Sage.

Gross, R., & Acquisti, A. (2005). *Information revelation and privacy in online social networks.* Paper presented at the Proceedings of the 2005 ACM workshop on Privacy in the electronic society.

Hajli, N., & Lin, X. (2014). Exploring the Security of Information Sharing on Social Networking Sites: The Role of Perceived Control of Information. *Journal of Business Ethics*. doi:10.1007/s10551-014-2346-x

Hann, I.-H., Hui, K.-L., Lee, S.-Y. T., & Png, I. P. (2007). Overcoming online information privacy concerns: An information-processing theory approach. *Journal of Management Information Systems, 24*(2), 13-42.

Hélou, C., Guandouz, A., & Aïmeur, E. (2012). A privacy awareness system for facebook users. *Journal of Information Security Research, 31*, 15-29.

Hew, K. F. (2011). Students' and teachers' use of Facebook. *Computers in Human Behavior, 27*(2), 662-676.

Hinduja, S. (2004). Theory and policy in online privacy. *Knowledge, Technology & Policy, 17*(1), 38-58.

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

Israel, G. D. (1992). *Determining sample size*: University of Florida Cooperative Extension Service, Institute of Food and Agriculture Sciences, EDIS.

Jackling, B., Natoli, R., Siddique, S., & Sciulli, N. (2014). Student attitudes to blogs: a case study of reflective and collaborative learning. *Assessment & Evaluation in Higher Education, 40*(4), 542-556. doi:10.1080/02602938.2014.931926

Jenkins, T. (2015). Public names have no right to be forgotten. Retrieved from http://www.scotsman.com/news/tiffany-jenkins-public-names-have-no-right-to-be-forgotten-1-3898832

Johnson, L. K., Aldrich, R. J., Moran, C., Barrett, D. M., Hastedt, G., Jervis, R., . . . Wark, W. K. (2014). An INS Special Forum: Implications of the Snowden Leaks. *Intelligence and National Security, 29*(6), 793-810. doi:10.1080/02684527.2014.946242

Joinson, A., Reips, U.-D., Buchanan, T., & Schofield, C. B. P. (2010). Privacy, Trust, and Self-Disclosure Online. *Human-Computer Interaction, 25*(1), 1-24. doi:10.1080/07370020903586662

Kang, T., & Kagal, L. (2010). *Enabling Privacy-Awareness in Social Networks.* Paper presented at the AAAI Spring Symposium: Intelligent Information Privacy Management.

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human-Computer Studies, 71*(12), 1163-1173. doi:http://dx.doi.org/10.1016/j.ijhcs.2013.08.016

Kim, S. H., Wang, Q.-H., & Ullrich, J. B. (2012). A comparative study of cyberattacks. *Communications of the ACM, 55*(3), 66-73.

King, G. (2014). EU 'right to be forgotten' ruling will corrupt history. Retrieved from https://cpj.org/blog/2014/06/eu-right-to-be-forgotten-ruling-will-corrupt-histo.php

Knijnenburg, B. P., Kobsa, A., & Jin, H. (2013). Counteracting the negative effect of form auto-completion on the privacy calculus.

Kotrlik, J., & Higgins, C. (2001). Organizational research: Determining appropriate sample size in survey research appropriate sample size in survey research. *Information technology, learning, and performance journal, 19*(1), 43.

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: why we disclose. *Journal of Information Technology, 25*(2), 109-125.

Kshetri, N. (2014). Big data′s impact on privacy, security and consumer welfare. *Telecommunications Policy, 38*(11), 1134-1145. doi:http://dx.doi.org/10.1016/j.telpol.2014.10.002

Ku, Y.-C., Chen, R., & Zhang, H. (2013). Why do users continue using social networking sites? An exploratory study of members in the United States and Taiwan. *Information & Management, 50*(7), 571-581. doi:http://dx.doi.org/10.1016/j.im.2013.07.011

Lai, I. K. W., Tong, V. W. L., & Lai, D. C. F. (2011). Trust factors influencing the adoption of internet-based interorganizational systems. *Electronic Commerce Research and Applications, 10*(1), 85-93. doi:http://dx.doi.org/10.1016/j.elerap.2010.07.001

Larson, R. G. (2013). Forgetting the First Amendment: How Obscurity-Based Privacy and a Right to Be Forgotten Are Incompatible with Free Speech. *Communication Law and Policy, 18*(1), 91-120. doi:10.1080/10811680.2013.746140

Lee, M.-C. (2009). Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit. *Electronic Commerce Research and Applications, 8*(3), 130-141. doi:http://dx.doi.org/10.1016/j.elerap.2008.11.006

Lee, M. (2008). *Predicting behavioral intention to use online banking.* Paper presented at the Proceedings of the 19th international conference on information management. Taiwan.

Li, H., Sarathy, R., & Xu, H. (2011). The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems, 51*(3), 434-445.

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems, 54*(1), 471-481. doi:http://dx.doi.org/10.1016/j.dss.2012.06.010

Li, Y., Stewart, W., Zhu, J., Ni, A., & Rohm Jr, C. (2012). Online Privacy Policy of the Thirty Dow Jones Corporations: Compliance with FTC Fair Information Practice Principles and Readability Assessment. *Communications of the IIMA, 12*(3), 65.

Lin, K.-Y., & Lu, H.-P. (2011). Why people use social networking sites: An empirical study integrating network externalities and motivation theory. *Computers in Human Behavior, 27*(3), 1152-1161. doi:http://dx.doi.org/10.1016/j.chb.2010.12.009

Lin, S.-W., & Liu, Y.-C. (2012). The effects of motivations, trust, and privacy concern in social networking. *Service Business, 6*(4), 411-424. doi:10.1007/s11628-012-0158-6

Lo, J. (2010). *Privacy Concern, Locus of Control, and Salience in a Trust-Risk Model of Information Disclosure on Social Networking Sites.* Paper presented at the AMCIS.

Madden, M. (2014). Public perceptions of privacy and security in the post-snowden era. *Pew Research Internet Project*.

Malandrino, D., Petta, A., Scarano, V., Serra, L., Spinelli, R., & Krishnamurthy, B. (2013). Privacy awareness about information leakage. 279-284. doi:10.1145/2517840.2517868

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

Manjoo, F. (2015). 'Right to Be Forgotten' Online Could Spread. Retrieved from http://www.nytimes.com/2015/08/06/technology/personaltech/right-to-be-forgotten-online-is-poised-to-spread.html?_r=0

Mantelero, A. (2013). The EU Proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten'. *Computer Law & Security Review, 29*(3), 229-235. doi:http://dx.doi.org/10.1016/j.clsr.2013.03.010

Martin, K. (2015). Understanding Privacy Online: Development of a Social Contract Approach to Privacy. *Journal of Business Ethics*. doi:10.1007/s10551-015-2565-9

Mayer-Schönberger, V. (2011). *Delete: the virtue of forgetting in the digital age*: Princeton University Press.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of management review, 20*(3), 709-734.

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

Merriam-Webster. (2015). Trust. Retrieved from http://www.merriam-webster.com/dictionary/trust

Mesch, G. S. (2012). Is online trust and trust in social institutions associated with online disclosure of identifiable information online? *Computers in Human Behavior, 28*(4), 1471-1477. doi:http://dx.doi.org/10.1016/j.chb.2012.03.010

Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing, 18*(3), 15-29. doi:10.1002/dir.20009

Min, J., & Kim, B. (2014). 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*.

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

Minkkinen, M. (2015). Futures of privacy protection: A framework for creating scenarios of institutional change. *Futures, 73*, 48-60. doi:http://dx.doi.org/10.1016/j.futures.2015.07.006

Mohamed, N., & Ahmad, I. H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior, 28*(6), 2366-2375. doi:http://dx.doi.org/10.1016/j.chb.2012.07.008

Morgan, L. (2015). List of data breaches and cyber attacks in August. Retrieved from http://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-august-2/

Morosan, C., & DeFranco, A. (2015). Disclosing personal information via hotel apps: A privacy calculus perspective. *International Journal of Hospitality Management, 47*(0), 120-130. doi:http://dx.doi.org/10.1016/j.ijhm.2015.03.008

Mundie, C. (2014). Privacy Pragmatism; Focus on Data Use, Not Data Collection. *Foreign Aff., 93*, 28.

Mvungi, B., & Iwaihara, M. (2015). Associations between privacy, risk awareness, and interactive motivations of social networking service users, and motivation prediction from observable features. *Computers in Human Behavior, 44*, 20-34. doi:10.1016/j.chb.2014.11.023

Narayanan, A., & Shmatikov, V. (2010). Myths and fallacies of "personally identifiable information". *Communications of the ACM, 53*(6), 24. doi:10.1145/1743546.1743558

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *The Journal of Consumer Affairs, 41*(1), 100-126. doi:10.2307/23860016

Olivero, N., & Lunt, P. (2004). Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control. *Journal of Economic Psychology, 25*(2), 243-262.

Oxford Online Dictionary. (2015). Awareness. Retrieved from http://www.oxforddictionaries.com/definition/english/awareness

Patagonia. (2015). The Footprint Chronicles. Retrieved from http://www.patagonia.com/us/footprint

Peters, J. (2015). The Reporters Committee and US media groups join the fight over 'right to be forgotten' rules. Retrieved from http://www.cjr.org/united_states_project/the_reporters_committee_and_us_media_groups_join_the_fight_over_right_to_be_forgotten_rules.php

Poslad, S. (2011). *Ubiquitous computing: smart devices, environments and interactions*: John Wiley & Sons.

Pötzsch, S. (2009). Privacy awareness: A means to solve the privacy paradox? *The future of identity in the information society* (pp. 226-236): Springer.

Preibusch, S. (2013). Guide to measuring privacy concern: Review of survey and observational instruments. *International Journal of Human-Computer Studies, 71*(12), 1133-1143.

Rees, C., & Heywood, D. (2014). The 'right to be forgotten' or the 'principle that has been remembered'. *Computer Law & Security Review, 30*(5), 574-578. doi:http://dx.doi.org/10.1016/j.clsr.2014.07.002

Rosen, J. (2012). The right to be forgotten. *Stanford law review online, 64*, 88.

Saunders, M., & Lewis, P. (2012). *Doing research in business and management: An essential guide to planning your project*: Financial Times Prentice Hall.

Saunders, M. N. K., & Bezzina, F. (2015). Reflections on conceptions of research methodology among management academics. *European Management Journal*. doi:http://dx.doi.org/10.1016/j.emj.2015.06.002

Schwartz, P. M., & Solove, D. J. (2011). PII Problem: Privacy and a New Concept of Personally Identifiable Information, The. *NYUL Rev., 86*, 1814.

Sekaran, U., & Bougie, R. (2010). Research methods for business: A skill building approach. Wiley: London.

Sharma, S., & Crossler, R. E. (2014). Disclosing too much? Situational factors affecting information disclosure in social commerce environment. *Electronic Commerce Research and Applications, 13*(5), 305-319. doi:http://dx.doi.org/10.1016/j.elerap.2014.06.007

Shleifer, A. (2012). Psychologists at the Gate: A Review of Daniel Kahneman's "Thinking, Fast and Slow". *Journal of Economic Literature, 50*(4), 1080-1091.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *Mis Quarterly, 35*(4), 989-1016.

Stutzman, F., Capra, R., & Thompson, J. (2011). Factors mediating disclosure in social network sites. *Computers in Human Behavior, 27*(1), 590-598. doi:10.1016/j.chb.2010.10.017

Sukamolson, S. (2012). Fundamentals of quantitative research. *Retrieved on, 25*.

Sun, Y., Wang, N., Shen, X.-L., & Zhang, J. X. (2015). Location information disclosure in location-based social network services: Privacy calculus, benefit structure, and gender differences. *Computers in Human Behavior, 52*, 278-292. doi:10.1016/j.chb.2015.06.006

Sutanto, J., Palme, E., Tan, C.-H., & Phang, C. W. (2013). Addressing the personalization-privacy paradox: an empirical assessment from a field experiment on smartphone users. *Mis Quarterly, 37*(4), 1141-1164.

Taddei, S., & Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure? *Computers in Human Behavior, 29*(3), 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), 248-273. doi:10.1111/jcc4.12052

Tan, X., Qin, L., Kim, Y., & Hsu, J. (2012). Impact of privacy concern in social networking web sites. *Internet Research, 22*(2), 211-233. doi:10.1108/10662241211214575

Trepte, S., & Reinecke, L. (2013). The reciprocal effects of social network site use and the disposition for self-disclosure: A longitudinal study. *Computers in Human Behavior, 29*(3), 1102-1112. doi:http://dx.doi.org/10.1016/j.chb.2012.10.002

Tucker, C. E. (2012). The economics of advertising and privacy. *International Journal of Industrial Organization, 30*(3), 326-329. doi:http://dx.doi.org/10.1016/j.ijindorg.2011.11.004

Tufekci, Z. (2007). Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites. *Bulletin of Science, Technology & Society, 28*(1), 20-36. doi:10.1177/0270467607311484

Tustin, D., Ligthelm, A., Martins, J., & Van Wyk, H. d. J. (2005). *Marketing research in practice*: Unisa Press Pretoria.

Uma, S., & Roger, B. (2003). Research methods for business: A skill building approach. *John Wiley and Sons Inc., New York*.

Ustaran, E. (2014). The wider effect of the 'right to be forgotten' case. *Privacy & Data Protection, 14*(8), 8-10.

Utz, S., & Krämer, N. (2009). The privacy paradox on social network sites revisited: The role of individual characteristics and group norms. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 3*(2), 2.

Väänänen-Vainio-Mattila, K., Wäljas, M., Ojala, J., & Segerståhl, K. (2010). *Identifying drivers and hindrances of social user experience in web services.* Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.

Venkatanathan, J., Kostakos, V., Karapanos, E., & Gonçalves, J. (2013). Online Disclosure of Personally Identifiable Information with Strangers: Effects of Public and Private Sharing. *Interacting with Computers*, iwt058.

von Solms, S., & van Heerden, R. (2015). *The Consequences of Edward Snowden NSA Related Information Disclosures.* Paper presented at the Iccws 2015-The Proceedings of the 10th International Conference on Cyber Warfare and Security.

Wakefield, R. (2013). The influence of user affect in online information disclosure. *The Journal of Strategic Information Systems, 22*(2), 157-174. doi:http://dx.doi.org/10.1016/j.jsis.2013.01.003

Wang, Y. D., & Emurian, H. H. (2005). An overview of online trust: Concepts, elements, and implications. *Computers in Human Behavior, 21*(1), 105-125. doi:http://dx.doi.org/10.1016/j.chb.2003.11.008

Warso, Z. (2013). There's more to it than data protection – Fundamental rights, privacy and the personal/household exemption in the digital age. *Computer Law & Security Review, 29*(5), 491-500. doi:http://dx.doi.org/10.1016/j.clsr.2013.07.002

Weber, R. H. (2010). Internet of Things – New security and privacy challenges. *Computer Law & Security Review, 26*(1), 23-30. doi:http://dx.doi.org/10.1016/j.clsr.2009.11.008

Weber, R. H. (2011). The right to be forgotten. *More than a Pandora's Box, 2*.

Westin, A. F. (1968). Privacy and freedom. *Washington and Lee Law Review, 25*(1), 166.

Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues, 59*(2), 431-453.

Whitman, J. Q. (2004). The two western cultures of privacy: dignity versus liberty. *Yale Law Journal*, 1151-1221.

Wolf, B. (2014). Free Speech versus Human Dignity: Comparative Perspectives on Internet Privacy. *Tul. J. Int'l & Comp. L., 23*, 251-283.

Woo, J. (2006). The right not to be identified: privacy and anonymity in the interactive media environment. *new media & society, 8*(6), 949-967.

Wright, K. B. (2005). Researching Internet-Based Populations: Advantages and Disadvantages of Online Survey Research, Online Questionnaire Authoring Software Packages, and Web Survey Services. *Journal of Computer-Mediated Communication, 10*(3), 00-00. doi:10.1111/j.1083-6101.2005.tb00259.x

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

Xu, F., Michael, K., & Chen, X. (2013). Factors affecting privacy disclosure on social network sites: an integrated model. *Electronic Commerce Research, 13*(2), 151-168. doi:10.1007/s10660-013-9111-6

Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the formation of individual's privacy concerns: toward an integrative view. *ICIS 2008 Proceedings*, 6.

Xu, H., Luo, X., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems, 51*(1), 42-52. doi:http://dx.doi.org/10.1016/j.dss.2010.11.017

Young, A. L., & Quan-Haase, A. (2013). Privacy Protection Strategies on Facebook. *Information, Communication & Society, 16*(4), 479-500. doi:10.1080/1369118x.2013.777757

Zikmund, W., Babin, B., Carr, J., & Griffin, M. (2012). *Business research methods*: Cengage Learning.

Zimmer, J. C., Arsal, R. E., Al-Marzouq, M., & Grover, V. (2010). Investigating online information disclosure: Effects of information relevance, trust and risk. *Information & Management, 47*(2), 115-123. doi:http://dx.doi.org/10.1016/j.im.2009.12.003

Zittrain, J. (2014). The right to be forgotten ruling leaves nagging doubts. Retrieved from http://www.ft.com/intl/cms/s/0/c5d17a80-0910-11e4-8d27-00144feab7de.html#axzz3Y5IIrrDe