

Gordon Institute of Business Science

University of Pretoria

Will the use of a third-party privacy seal (lock) in an e-mail advertisements result in a higher likelihood of consumers disclosing their private information?

Lee Zuk

14448166

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

09 November 2015

ABSTRACT

One of the commodities in the commercial world has become access to data, specifically personal information. The Internet has rapidly expanded a company's ability to access consumers' and individuals' personal information, however consumers' privacy-concerns regarding the disclosure of their personal information have continued to increase. Using an e-mail marketing campaign, this research explored the impact of using third-party privacy seal (lock) as signals to facilitate consumers disclosing private information.

The study employed a live experimental randomised two-group post-test only design, whereby an e-mail advertisement, identical in design except for the image of a third party seal (lock) placed on the non-control group's e-mail. The test explored whether the e-mail advertisement containing the third-party privacy signal (lock) had an impact on whether or not the recipient behaved in a certain way in comparison to the e-mail advertisement that did not contain a lock.

The results showed no real significant difference of the third-party seal (lock) on the consumer's preparedness to disclose personal information. Whilst the lock may be used as a trust symbol it is not enough, within the online advertising context, to entice disclosure of personal information. To remain competitive, companies will need to reassess their advertising strategies and further research will need to identify high value signals to encourage consumer disclosure.

Keywords

Privacy, consumer disclosure, online advertising, e-mail advertising, third-party seal.

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.

Lee Zuk

09 November 2015

CONTENTS

Abstract	2
Declaration	3
Contents	4
CHAPTER 1.....	8
1 Introduction To The Research Problem	8
1.1 Research Title	8
1.2 The Research Problem.....	8
1.2.1 <i>Introduction</i>	8
1.2.2 <i>Background to consumer privacy consumers, personal information and disclosure</i>	9
1.2.3 <i>Background to third-party privacy seals (lock)</i>	11
1.3 Research Objectives	12
1.4 Research Aim and Motivation.....	13
CHAPTER 2.....	14
2 Literature Review	14
2.1 The Formation of the Concept – Information Privacy	14
2.1.1 <i>Defining private information</i>	14
2.1.2 <i>Information privacy on the Internet</i>	15
2.2 Internet Advertising and Consumer Behaviour	19
2.2.1 <i>Consumers’ response to advertising online</i>	19
2.2.2 <i>Companies’ advertising strategies surrounding consumer privacy concerns</i>	21
2.3 Trust	23
2.3.1 <i>The role of trust as a component of information privacy</i>	23
2.3.2 <i>Trust and online advertising</i>	23
2.4 Signalling Theory	25
2.4.1 <i>Introduction of signalling theory</i>	25
2.4.2 <i>Signalling theory in the online marketing context</i>	27
2.4.3 <i>Third-party seals, signalling theory and privacy concerns</i>	30

2.5	Consumer Disclosure of Private Information	31
2.5.1	<i>The private nature of disclosing income</i>	31
2.5.2	<i>Do different demographics disclose private information differently?</i>	32
CHAPTER 3	35
3	Research Hypotheses	35
3.1	Introduction	35
3.2	Hypotheses.....	35
3.2.1	<i>Hypothesis 1</i>	35
3.2.2	<i>Hypothesis 2:</i>	36
3.2.3	<i>Hypothesis 3:</i>	36
3.2.4	<i>Hypothesis 4:</i>	36
CHAPTER 4	38
4	Research Methodology	38
4.1	Introduction	38
4.2	Research Design	38
4.2.1	<i>Validity of the research</i>	40
4.3	Universe	41
4.4	Sampling Method and Size.....	42
4.5	Unit of Analysis.....	44
4.6	Data Gathering	44
4.7	Data Analysis.....	45
4.8	Limitations	46
CHAPTER 5	48
5	Results	48
5.1	Descriptive Data	48
5.2	Inferential statistics for each hypothesis	49
5.2.1	<i>Hypothesis 1</i>	49
5.2.2	<i>Hypothesis 2</i>	52
5.2.3	<i>Hypothesis 3</i>	55
5.2.4	<i>Hypothesis 4</i>	58

5.3 Summary of the results.....	62
CHAPTER 6.....	63
6 Discussion Of Results	63
6.1 Introduction.....	63
6.2 Summary	63
6.3 Hypothesis 1: A third-party privacy seal (lock) is a high value signal, and will result in consumer disclosure.....	64
6.4 Hypothesis 2: A third-party privacy seal (lock) will result in a higher click-through rate on an e-mail advertisement	67
6.5 Hypothesis 3: Desktop, Mobile and Tablet	69
6.6 Hypothesis 4: Gender differences	72
6.7 Conclusion.....	76
CHAPTER 7.....	77
7 Conclusion.....	77
7.1 Introduction.....	77
7.2 Findings	77
7.3 Recommendations	78
7.4 Managerial Implications.....	80
7.5 Limitations of the research and suggestions for future research	80
7.6 Conclusion.....	81
Reference List	83
Appendices.....	89
Appendix A - E-mail AdvertisEment Group A	89
APPENDIX B - E-mail AdvertisEment Group b.....	90
APPENDIX C - Group A and b website.....	91
Appendix D – Ethical clearance Approval	92

Appendix E – Turnitin report 93

CHAPTER 1

1 INTRODUCTION TO THE RESEARCH PROBLEM

1.1 Research Title

Will the use of a third-party privacy seal (lock) in an e-mail advertisements result in a higher likelihood of consumers disclosing their private information?

1.2 The Research Problem

1.2.1 Introduction

“Personal data is the new oil of the Internet and the currency of the digital world” (Spiekermann, Acquisti, Böhme & Hui, 2015).

This research examines whether the use of a third-party privacy seal (a lock), in a company’s e-mail advertisement, can generate consumers’ disclosure of their personal/private data (personal information). While there has been research within the academia surrounding privacy concerns, the links between trust mediating effects of privacy concerns and personal information online disclosure have been suggested as requiring further exploration (Mothersbaugh, Foxx, Beatty & Wang, 2012, p.16).

This research seeks to answer the call by Mothersbaugh et al. (2012). As a method of exploration, the research looked at signalling theory. Signalling theory has identified ways for companies to relieve consumers’ concerns and vulnerabilities within the context of personal information (Liberali, Urban & Hauser, 2013). For example, the brand itself has been identified as one of the signals eliciting trust (Liberali et al., 2013). Brand credibility, operationalised as trustworthiness and expertise, was found to be a useful signal aimed at increasing brand consideration (Liberali et al., 2013).

The increasing concerns consumers have surrounding the collection, storage and usage of their private information also has an impact on a company’s ability to access personal

information of their consumers. It is vital that companies gain consumer trust in eradicating privacy concerns. Moreover, the previous literature regarding signalling theory, has further identified that using a third-party privacy seal is a 'high-quality' signal that is effective in alleviating consumer privacy concerns (Liberali et al., 2013).

1.2.2 Background to consumer privacy consumers, personal information and disclosure

While the free-flow of information created by the Internet has rapidly expanded a company's ability to access consumers' and individuals' personal information, the vast information asymmetries that exist online, have left consumers feeling vulnerable, and caused continuous increase for consumers' privacy-concerns regarding the use of their personal information (Goldfarb & Tucker, 2012; Roeber, Rehse, Knorrek & Thomsen, 2015; Edelman Trust Barometer, 2015; Spiekerman et al, 2015). "Lawsuits against popular websites (e.g., Google Buzz, Facebook, Beacon and AOL Value Click) for violation of online privacy, and the implementation of online Privacy Protection Acts (e.g., the Federal Trade Commission of 2007), are evidence of the increased importance and interest in online privacy" (Hong, 2013, p.276). The research seeks to add to the growing body of knowledge in this area.

In June 2015, it was reported that there are over 3 billion Internet users globally (a substantial increase from the 2010 statistic of 360 million users) and when measured as a separate industry in 2012, the Internet industry was already a larger contributor towards GDP than the Federal Government in the United States of America, as well as among China's and South Korea's top six industry sectors (Dean, DiGrande, Field, Lundmark, O'Day, Pineda & Zwillenberg, 2012).

Companies around the globe are rapidly employing the Internet as a business medium as well as a communication channel with their consumers. Forrester's 2014 research report statistics revealed that companies are rapidly increasing their Internet marketing spend – which is predicted to "top \$103 billion in 2019, up from \$57.3 billion this year" (Forrester, 2014), furthering the need to research the advertising returns obtained by companies spending such large budgets.

Globally, individuals receive 196 billion e-mails daily, submit over 500 million tweets and

share 4.75 billion pieces of content on the social media platforms (Spiekermann et al., 2015, p.161). While it is therefore evident that consumers are sharing personal information on the Internet, the effect of online consumers' privacy concerns has caused “drop-off rates (That is people who display intention to purchase, but then do not purchase) at the point of purchase at online stores to be higher than the drop-off rates at offline stores” (Kim & Kim, 2011, p.146). Therefore, it is pertinent that both Internet-based companies and the companies using Internet as a channel for growth are able to access their consumers' personal information in a way that will not inhibit them '.

The Internet has lowered the barriers to global entry for companies, and companies need to ensure their consumers do not drop off. And there is a further need to manage personal information, when accessed, in a way that ensures consumers are not left feeling vulnerable and out of control, in order to remain competitive and serve customers efficiently (Aguirre, Mahr, Grewal, Ruyter & Wetzels, 2015).

The rapid growth of the Internet, the commoditisation of privacy online, and rapid technological advances of online advertising through social and search platforms including Google, Twitter and Facebook (Xu, Luo, Carroll & Rosson, 2011) have produced a clear channel for the growth of companies and direct and immediate access to consumers.

Consumer privacy concerns regarding data collection and usage have been prominent topics within academia, and the findings have shown that consumers resist both Internet commerce and the adoption of new technologies, in the presence of significant privacy concerns (Xu, Teo, Tan & Agarwal, 2012). As a result, governments worldwide have implemented information privacy acts, in an attempt to protect their citizens' fundamental privacy rights. Privacy violations seem abundant, as reflected by the plethora of lawsuits launched by individuals against the top Internet companies for violation of consumers' online privacy (Hong, 2013, p.276).

Due to the obvious competitive advantage gained by companies who successfully access consumer's private information, researchers have been examining ways to address consumer privacy and trust concerns. The existing research has, inter alia, examined the topic in light of advertising practices and data collection. The obtuse and covert online advertising practices used by companies for the collection of private information have

been identified as exploiting private and personal consumer information and as a “predominant trigger” of consumers’ privacy and trust concerns online (Bleier & Eisenbeiss, 2015, p.6). John, Acquisti and Loewenstein (2011) called for further research to identify the conditions that promote consumer disclosure decisions.

Özpolat and Jank (2015, p.47) disclosed that the latest TRUSTe 2014 US Consumer Confidence Index reported a 4% increase of consumers’ mistrust in online companies since its 2012 index. The 2015 annual Edelman Trust Barometer found that “nearly 63% of respondents would not buy products and services from companies and brands they did not trust and, conversely, a majority 80% would buy products and services from companies they trusted”.

1.2.3 Background to third-party privacy seals (lock)

There is a monetary and timeous cost in acquiring and maintaining the requirements for a third party seal, and the literature has identified that a third-party privacy seal is a high-cost signal, that is also easy to verify and therefore seen as one of high quality.

Mothersbaugh et al. (2012) called for further research of these signals in different contexts. E-mailed advertising had been identified in literature as being mistrusted and linked to consumer privacy risks due to their common identification as “spam” (Kim & Kim, 2011) and their research therefore identified e-mail advertising as needing further exploration.

The value and effectiveness of trust seals in e-commerce have been investigated by researchers in as tools to gain consumer trust online (Atkinson & Rosenthal, 2014; Kim & Kim, 2011; Özpolat & Jank, 2015; Xu et al., 2011). Aguirre et al. (2015, p.38) stated that the Internet Advertising Bureau UK (2011) urged companies to incorporate icons on their websites to “inform users about data collection and usage practices”, identifying that a third-party privacy seal (lock) “increase trust perceptions, goodwill and are integrity indicators, and show the behavioural intentions of the company”. Furthermore, third party seals can only be received from an independent certifying body, authorising industry standards as being upheld and companies can only use the seal if they are members of the industry body. This requires both monetary payment and technical requirements in

order to be authenticated (Mavlanova, Benbunan-Fich & Koufaris, 2012; Wells, Valacich & Hess, 2011). Özpolat and Jank (2015) suggested that while the use of seals has been researched, it is still underexplored and scarce with regard to contextual factors that facilitate the functioning of trust seals.

1.3 Research Objectives

The broad objective and fundamental question this research aimed to answer is whether a third party seal, when used as a signal in an e-mail advertisement, will influence consumers' behaviour, specifically in relation to disclosure of private information.

A South African online marketing company (JHY), that connects financial services partners with consumers looking for financial service products, was used for the purpose of the test. The data subjects (database) of company (JHY) that were used for the purpose of the study consisted of three brands that belonged to the company (JHY). These brands are referred to within the literature as Base J, Base H and Base Y for anonymity purposes. The company (JHY) relies on gathering consumer information for their financial services partners, using e-mail advertisements amongst many other marketing channels and therefore was identified as a relevant research environment for the study.

The study employed empirical evidence gathered from a live (real-time) experimental randomised two-group post-test e-mail advertisement sent to the JHY database in order to ascertain:

- Whether the third party seal is used in an e-mail advertisement does in fact positively impact consumer disclosure of personal information.

The main research question is whether a third party seal is a strong enough signal for companies to use online in order to impact consumer behaviour and entice disclosure of their personal information.

1.4 Research Aim and Motivation

This research aimed to examine the use of third-party seals (lock) as a signal to consumers that it is safe to disclose personal information to a company.

Companies seek to obtain private information from consumers for several business purposes (profit seeking, offering better services, connecting with relevant consumers and saving on costs) and rely on consumers' voluntary disclosure of private information in order to utilise the collected information legally. It is very important, within the online context, that consumers trust the companies they disclose information to, to re-use the information fairly, legally and legitimately, and further to do this in a way that new consumers identify them as high-quality trustworthy companies.

The Internet is growing globally and as such, the study provides information useful to other companies in South Africa who are growing online about whether the use of third-party seals, is a high value signal as described in markets that are already developed. It also provides information that is useful for companies within South Africa.

The research also looked to improve advertising marketing ROI (return on investment) by empirically studying whether using third-party privacy seals (lock) in an e-mail advertisement results in a higher likelihood of consumers disclosing their private information.

CHAPTER 2

2 LITERATURE REVIEW

2.1 The Formation of the Concept – Information Privacy

2.1.1 Defining private information

For the purpose of this research, private information will refer to “information relating to an identifiable, living, natural person”, as defined by The South African Protection of Personal Information Act No.4 of 2013 (POPI). POPI defined private information broadly extending the ambit of its meaning to include eight category types ranging from basic demographics of race and gender, to individual views and preferences. All these categories relate to the personal data that can be used to identify an individual.

Little consensus exists in literature as to what exactly the definition of privacy is (Kim & Kim, 2011; Tucker, 2012; Pavlou, 2011). Early research on privacy simply described solving of privacy concerns as a matter of giving an individual control over their own data (Tucker, 2012). Bleier and Eisenbeiss (2015, p.6) extended the description to “the ability of the individual to control the terms under which their personal information is acquired and used”. Smith, H. J., Dinev, T. & Xu, H. (2011, p.995) stated that if such a definition is viewed only as a state of control, and considered in terms of its single “role as a sought-after goal”, this limited its true definition. They suggested that researchers should rather regard privacy more as a class of multifaceted interests. Moreover, Smith et al. (2011) recommended that these multifaceted-interests must to be contextualised before they can be defined.

Therefore, given the focus of this research, privacy will be discussed within the context of Internet (online) marketing and advertising literature relating to personal information.

2.1.2 Information privacy on the Internet

Melena Konev's words that "personal data is the new oil of the Internet and the currency of the digital world", have been repeated frequently within the literature (Spiekermann, Acquisti, Böhme, & Hui, 2015). This identified the commoditisation of personal data that the Internet created which expanded a company's ability to access individuals' and consumers' private information (Quelch & Jocz, 2008; Aguirre et al., 2015). The digitalisation of personal information, through Internet technologies and social platforms, poses new challenges for the already existing "ethical, legal, social and political issue of the information age" (Hong, 2013, p.276).

While a company's ability to acquire consumers' personal information is therefore vital to its growth and strategy, continuing mistrust and privacy concerns of online consumers is increasing. New technical modifications, such as new privacy-browsing modes, and the ever-growing global legislation protecting information privacy online have exacerbated these concerns and mistrusts, and therefore a company's ability to use, store and manage this private information is just as vital, if not essential to its survival and competitive advantage (Acquisti, John & Loewenstein, 2013; Mothersbaugh et al., 2012; Tsai, Egelman, Cranor & Acquisti, 2011).

It is essential to understand that the company and the consumer face different dilemmas regarding private information and the disclosure thereof. The consumer and the company have differing needs for private information, and it is the way this information is used and disclosed that impacts on the objectives of this study and are therefore expanded on below.

2.1.2.1 *The context of the company*

The context of the company focuses on gaining access to personal information. The free-flow of knowledge is essential to a well-functioning consumer marketplace and the Internet has increasingly expanded a company's ability to access, individuals' private information (Quelch & Jocz, 2008; Aguirre et al., 2015), identified as an asset in today's global economy (Spiekermann et al., 2015, p. 161).

The sharing of personal information is evident on the Internet (Spiekermann et al., 2015, p.161) and a company's, access, collection and usage of this shared information can be a major competitive advantage but also an inevitable necessity for the survival of companies (Aguirre et al., 2015; Spiekermann, Acquisti, Böhme & Hui, 2015), functioning within a marketplace where information is, as Konev (2009) stated, a form of "currency of the digital world" (Spiekermann, Acquisti, Böhme & Hui, 2015) for the company and the consumer.

2.1.2.2 The context of the consumer

The literature has studied several challenges that exist for consumers surrounding their apprehension for sharing data on the Internet (online). While more consumers are choosing to share their personal information online (Spiekerman et al., 2015), an individual's mistrust surrounding the appropriate use of their data has continued to grow over the years (Tucker, 2012; Roeber et al, 2015). In a recent study, Tucker (2012, pg.327) identified that as many as 86% of young adults do not want to receive personalised and targeted advertisements, as they do not trust that the company that has collected the information will use it for the purposes that it is expressing. This is corroborated by the increase in legal restrictions and boundaries relating to companies access, usage and finally ethical boundaries of consumers' private information (Tucker, 2012; Spiekerman et al., 2015; Kim, 2011 & Bandyopdhyay, 2009).

These consumer concerns have made it challenging for advertisers to communicate to and with consumers, and to gain consumer trust or to advertise to them by using personal (private) information the consumer had previously disclosed.

2.1.2.3 Context and consumer disclosure

The role of context has an impact on the consumer's assessment and valuation of their private information (Pavlou, 2011). Smith et al. (2011, p.1002) made reference to Mowday and Sutton's (1993) definition of context to refer to "stimuli and phenomena that surround and thus exist in the environment external to the individual, most often at a different level of analysis". Within this understanding of context the research has assumed that the

valuation of private information is linked to both external and internal stimuli within the environment of the consumer, who, as described by Aguirre et al. (2015, p.37) is a “rational economic agent” that cognitively assesses the risks and benefits in disclosing their private information.

Smith et al. (2011) proposed that the context for privacy includes, *inter alia*, the type of information collected from individuals, which are often referred to as contextual sensitivity or information sensitivity. Consumers’ beliefs and behavioural responses to privacy threats depend on the type of information being requested (Goldfarb & Tucker, 2012; Xu et al., 2011). The academic literature has found it challenging to identify how disclosure of private information as well as privacy concerns have changed, due to the fact that the frequency of opportunity for people to reveal information has grown so rapidly with the expansion of the Internet (Goldfarb & Tucker, 2011).

Throughout the literature it is evident that different contexts elicited differing impacts on consumers’ disclosure. Mothersbaugh et al. (2012) referred to the sensitive nature of private information. They suggested that there is a vulnerability created for consumers in divulging personal data due to consumer’s perceptions that sensitive information is riskier to share. This was also highlighted in a study by Goldfarb & Tucker (2012), where data subjects revealed less information in a survey as time passed, because of the nature of the requested information. Goldfarb & Tucker (2012) concluded that – as the information being requested became more sensitive – the respondents revealed less information in the more privately sensitive context of a survey than in the less privately sensitive context. Multidimensional development theory helped to develop the concept and context of disclosing information and consumer privacy concerns.

2.1.2.4 *Multidimensional developmental theory*

Laufer and Wolfe’s (1977) initial multidimensional developmental theory (MDT) stated that privacy concerns are a “result of self-development, environmental impact, and, most importantly, interpersonal interaction. Hong (2013, p.277) identified the interpersonal interaction as constituting the core of consumers’ online privacy concerns because it indicates the “existence” of another concern within their context of the concern. For the consumer, this means that their privacy concerns exist only because of their relationship

between them and another party (the computerised programme, website or advertisement). If not for that other party, the concerns surrounding the relationship they have with the party would not exist.

Hong (2013, p.77) suggested two management functions, which are core to interpersonal interaction for consumers, namely “interaction management and information management”. The first function, interaction management refers to the way a person responds to the experience with the other. Online this is a computerised experience, which is therefore intangible for the consumer. This experience has made it difficult for consumers to know if what one sees online (i.e. what is displayed by the company) is in fact exactly what one is buying. The response by consumers to this intangible “other party” within the online context has been linked to the fundamental impulse of consumers to look for control within managing and disclosing their private information (Hong, 2013).

Individuals may not perceive themselves as having control over how computers manage their private or confidential information (Hong, 2013, p.279) and Hong wrote that various research studies, conducted between 2007 and 2009 (“by Buchanan et al. (2007); Culnan and Williams (2009); and Pavlou et al. (2007)”), identified concerns by online consumers, around how companies are managing their information online after it has been collected. This concern included the way their personal data is managed by websites (Hong, 2013, p.277).

The second management function, namely information management is linked to relationship between the company and the consumer. Lwin and Williams (2003) and more recently, Aguirre et al., (2015) suggested that the exchange of a consumer’s private information between them and a company sat within this concept of information management. This exchange being subject to a consideration of future consequences as well as weighing up the risks and benefits of whether or not to engage with the company. This consideration is identified as a disclosure determinant for consumers (Lwin and Williams, 2003, p.260). The obstacle for the company is their ability to gain access to individuals’ private information especially in light of consumers’ mistrust and privacy concerns. Spiekermann, Acquisti, Böhme and Hui (2015) highlighted the power companies have in helping to create an environment where the company manages a person’s concerns around their private information.

In other literature related to multidimensional development theory (MDT) , Lwin and Williams (2003) and Hong (2013) suggested that third-party certification are an effective tool for companies to use to assist information management, in order to ease consumers' concerns, making them feel more in control. Third-party certification allows consumers to measure websites' "intangible" qualities more objectively as a third-party certification signifies that a website's information practices are in line with industry privacy standards (Lwin and Williams 2003, pg.267) which gave a website a more "tangible" identifier for consumers.

In light of the interpersonal dimension of MDT, this research, therefore, investigated whether using a third-party certification on the advertisement, has the same effect as being used on a website and ultimately viewed as tool for the company's management of a consumers information management, to ease the consumers' concerns, giving them a sense of control. This may, in turn, result in a more likely chance of consumers disclosing their private information. The next section of the review looks further into the academic literature around advertising online and its impact on consumer behaviour.

2.2 Internet Advertising and Consumer Behaviour

Vast information asymmetries exist online, with the free-flow of information created by the Internet, leaving consumers feeling vulnerable. This is due to the constant online requests for personal information on the Internet and the ease with which anyone accesses vast amounts of personal information about others on various Internet platforms, creating a constant awareness for the consumer that their information is being captured with or without their consent (Acquisti, John & Loewenstein, 2012; Atkinson & Rosenthal, 2014; Kim & Kim, 2011).

2.2.1 Consumers' response to advertising online

Bleier and Esienbess (2015, p.6) identified the covert practice of firms collecting, analysing and exploiting private and personal consumer information through their advertising, which has been a "predominant trigger" of online consumers' private information dissemination and has been viewed by consumers as an intrusion and "a loss

of control”. This consumer vulnerability towards the company collecting data through and for advertising results in an inhibition in consumers disclosure due to its prompting of the consumers’ privacy concerns” (Bleier & Eisenbeiss, 2015, p.6).

The individual’s risk of losing the privacy of their personal information has been defined in research as “the degree to which an individual perceives a potential loss associated with personal information” (Pavlou, 2011, p.981), and has been proposed as an antecedent of information privacy concerns. While individuals express strong privacy concerns and an inhibition to disclose their personal information, consumers have consistently behaved in a contradictory manner, as they have previously and still continue to disclose their private information (Aguirre et al., 2015; Pavlou, 2011; Xu et al., 2011, 2011). This has been defined in the literature as a privacy paradox phenomenon (Pavlou, 2011; Xu et al., 2011). Consumers appreciate, while their data-sharing can lead to them only being exposed to and selected for products and services that “fit” their stated interests, an exchange exists and in this exchange, the risk of disclosing their private information needs to be worth the return (Tucker, 2012). Xu et al. (2011, p.44) described the privacy-paradox as “the individual’s overall assessment of the utility of information disclosure based on perceptions of privacy risks incurred and benefits received”. This paradox has been identified as a gap for companies to use in accessing personal information of consumers.

In more recent academic research, the privacy-paradox has been called a “relic of the past” (Dienlin & Trepte, 2015). Roeber et al. (2015) stated that an overwhelming majority of their data subjects were willing to share data with organisations, if the benefits and terms met their needs. Supporting this attitude is the study by Xu et al. (2011), which provided empirical evidence that a commoditisation of private information exists through showing that, giving monetary compensation and / or a value (i.e., a prize) to consumers can be regarded as enough of a benefit for consumers to disclose their information (Xu et al., 2011). While academic research, such as Dienlin & Trepte (2015), argued that commoditising private information means that consumer concern does not exist, or is not as extensive as has been alluded to, the objectives within this research investigated whether it is a relic of the past or in fact an addition to the dimensions of information privacy. As most of the previous academic studies verify a clear interpersonal dimension, describing the distinct existence of an interpersonal relationship resulting in privacy concern for consumers, the hypothesis for the research does view the paradox as real.

2.2.2 Companies' advertising strategies surrounding consumer privacy concerns

"Implicit in most of the neoclassical economics literature on privacy is the assumption that consumers are rationally informed agents with stable privacy preferences" (Acquisti, John & Lowenstein, 2013, p.253).

The marketing and advertising literature has tested consumer rationality in light of the privacy-paradox (White & Yuan, 2012; Atkinson & Rosenthal, 2014; Aguirre et al., 2015; Baek & Morimoto, 2012). Such studies endeavoured to combat the avoidant behaviour of consumers toward Internet advertising (Verlegh, Fransen & Kirmani, 2015), as well as the use of third-party certification and other schema in advertisements or on website pages, in order to gain consumer trust (Hu, Wu, Wu & Zhang, 2010; Kim & Kim, 2011). Marketers have been found to collaborate with major global publishers that have collected and who own mass data, such as Google and Facebook, to overcome successfully the privacy-paradox through personalisation of advertising (Aguirre et al., 2015).

Several studies have investigated and identified ways in which companies are addressing consumer privacy concerns, making their consumers feel more in control of their information. Tucker (2014), for example, conducted studies to identify whether the strengthening of privacy controls by a company affects consumers' choice to disclose their private information, therefore improving advertising performance. Previous academic studies showed that consumer privacy concerns were managed through the company in an explicit manner, visibly drawing the consumer attention to the fair procedure policies employed by the firm. These were managed successfully to the point that consumers overtly gave permission to companies to disclose their personal information to third party companies (Hann, Hui, Lee & Png, 2007; Miyazaki & Krishnamurthy, 2002; Tucker, 2014; Xu et al., 2011). Tucker (2014) implemented a field experiment and investigated whether increasing a consumer's control over their data on social media sites would help to manage their privacy concerns when responding to advertisements. Tucker (2014) chose to target social media as social media advertisements were identified in the research as having low click-through rates. These low click-through rates meant high costs for advertisers to reach consumers on a platform where the majority of their consumers were found. Their research found that consumers gained control over how their private

information was used and stored and this resulted in higher click-through rates across their experiment and therefore assisted advertisers on social networking sites.

Schemas were defined (Goodrich, 2014, p.33) as “ways in which consumers can more easily process information through categorisation and generalisation, providing a ‘shortcut’ cognitive framework to organise and interpret large amounts of information” Third-party seals (Locks) have also been identified in the electronic commerce literature to be strategic and effective tools in enhancing consumer trust toward a brand through managing consumers’ privacy concerns (Özpolat & Jank, 2015). Kim & Kim (2011, p.146) suggested that a third-party seal may be a more practically advantageous way for online businesses to gain consumer trust than the visibility of privacy policies because they are obvious schema that consumers use to judge objectively and trust a website.

Mothersbaugh et al. (2012) found that trust and disclosure of private information can be positively influenced through firms including particular elements on their websites, such as third-party seals, which have been seen in the research to result in consumers feeling less vulnerable in disclosing their private information, instantly identifying these as a signal that the website must be more trustworthy (Aguirre et al., 2015; Kim & Kim, 2011).

Previous research examined the consumer response to the use of their personal information within an advertisement targeted at them; its impacts on consumers’ trust levels, privacy concerns and purchasing behaviour (Bleier & Eisenbeiss, 2015; Tucker, 2014; Tucker, 2012; Van Doorn & Hoekstra, 2013). Van Doorn and Hoekstra (2013, p.339) found that, while online retailers can use customisation of advertisements advantageously to correspond with consumers’ contexts and needs, to increase their purchase intention, “it is a double-edged sword leading to higher purchase intentions, but also greater perceived intrusiveness, which then negatively affects purchase intentions”.

According to Bleier and Eisenbeiss (2015), the extent to which an advertisement generated privacy concerns depended on the sensitivity of the consumers’ personal information used within the advertisement. Bleier and Eisenbeiss (2015) used field data to examine the effectiveness of personalisation of advertising, through retargeting consumers with advertisements based on previous consumer activity and whether this level of personalisation considerably hinges on consumers’ trust in a particular retailer. In

both the Aguirre et al. (2015) and Bleier and Eisenbeiss (2015) studies, the impact of personalising advertisements was found to threaten consumers' feeling of vulnerability and heightened consumers' awareness of the data collecting, as well as the type of advertisement personalisation and usage of data. Aguirre et al. (2015) found that – if personal information was collected overtly – the effectiveness of the advert was higher than when collected overtly by a company, showing the consumers' feeling of vulnerability to how their information is gathered. Bleier and Eisenbeiss (2015) found that while the more trusted retailers benefitted from personalisation of advertisements, the converse was true for the less trusted retailer.

Trust has been identified as an interrelated variable of information privacy and can either be a precursor; consequence; and / or a successful mediator between information privacy and a consumer's willingness to disclose private information (Pavlou, 2011, p.981). Therefore, in managing the interpersonal dimension of privacy concerns, it is important that companies consider trust towards their company, their products or services. This is discussed in the next section of the literature review.

2.3 Trust

2.3.1 The role of trust as a component of information privacy

Aguirre et al. (2015, p.37) defined trust as an interpersonal “ psychological state, comprising the intention to accept vulnerability based on positive expectations of the intentions or behaviours of another”. Spiekerman et al. (2015) identified the need for businesses to ensure they create more trustworthy relationships with consumers, to counter-affect their feelings of vulnerability and privacy concerns. The management of trust by companies can be viewed as benefiting consumer's information management of their consumer interpersonal aspect of their privacy concerns (Hong, 2013).

2.3.2 Trust and online advertising

“On the Web, trust often serves as the sole foundation on which consumers base their research and purchase decisions because of lack of further information about firms” (Bleier & Eisenebiss, 2015, p.2). While literature has explored and found that when

companies gain consumer trust, it has a powerful positive impact for the consumer on the feeling of vulnerability towards the company that developed due to the available vast online information accessibility that exists online (Aguirre et al., 2015; Bleier & Eisenbeiss, 2015). There is also evidence in other research, which has found that when the company does not create consumer trust, the powerful impact on the consumers' feeling of vulnerability increases and inhibits disclosure (Leon, P. G., Ur, B., Wang, Y., Sleeper, M., Balebako, R., Shay, R. Bauer, L., Christodorescu, M., Cranor, L. F., 2013).

Atkinson and Rosenthal (2014) studied the impact of the content used in an advertising message and its influence on consumer trust. They found that if consumers do not trust the content of the marketing claims, or even merely suspect that claims are not true, they are much less likely to purchase from that company or engage with that advertisement (Atkinson & Rosenthal, 2014).

In 2015 The Edelman Trust Barometer, a barometer commonly used in various academic research studies (Liberali, et al., 2013; Smith, et al., 2011; Xu et al., 2011), found that “nearly two-thirds of respondents refuse to buy products and services from a company they do not trust. Conversely, 80 percent (80%) chose to buy products from companies they trust” (Spiekermann et al., 2015, p.165).

“The Internet Advertising Bureau UK (2011) urges firms to incorporate icons to inform users about data collection and usage practices because such icons could increase trust perceptions (Pan & Zinkhan 2006), benevolence and integrity beliefs (Schlosser, White & Lloyd 2006), and behavioural intentions (Wang, Beatty, & Foxx 2004)” (Aguirre et al., 2015, p.38). Academic research has found similar results and has found that, in the use of these behaviour-influencing strategies on their websites, marketers have been successful in gaining consumer trust online and in turn increase the consumer engagement with the brand (Aguirre et al., 2015; Kim & Kim, 2011; Mothersbaugh et al., 2012).

Privacy concerns have been mitigated or reduced, for example, through the use and implementation of fair information practices, displaying of privacy notices on a website and third-party seals, all of which had a noticeable positive effect on the consumers' perception of trust in a website, resulting purchase by consumers as well as increasing positive brand perception (Mothersbaugh et al., 2012; Smith et al., 2011). Studies were

recently conducted which explored the challenges of data markets, and the impact of exacerbating privacy concerns with significant relevance on companies' obligations and participation in the creation of consumer trust in order to tackle the legal, economic, technical and social challenges that privacy concerns are bringing (Spiekermann et al. 2015).

Kim & Kim (2011) used third-party seals to build consumers' trust on a website where a consumer had no previous knowledge of the retailer and found that there was, in fact, an increase in purchases. The results depicted in the study by Kim & Kim (2001) displayed that there is a transference of trust for consumers when a third-party seal is used on a website. It recommended that marketers use the empowering influence of third-party certification to build consumers' initial trust in retailer websites with which they have no prior experience (Kim & Kim, p.154).

Spiekermann et al. (2015, p.165) found that firms can achieve and increase a trustworthy relationship with customers through the use of upfront digital agreements (instead of covert agreements) with customers as these allow the consumers to know upfront what their private information will be used for and which information will be used.

Mothersbaugh et al. (2012, p. 16) concluded, "Trust mediates the effects of online privacy concerns and information control on disclosure". This linkage had not been explored by previous research and was recommended by Mothersbaugh as an avenue for future research.

2.4 Signalling Theory

2.4.1 Introduction of signalling theory

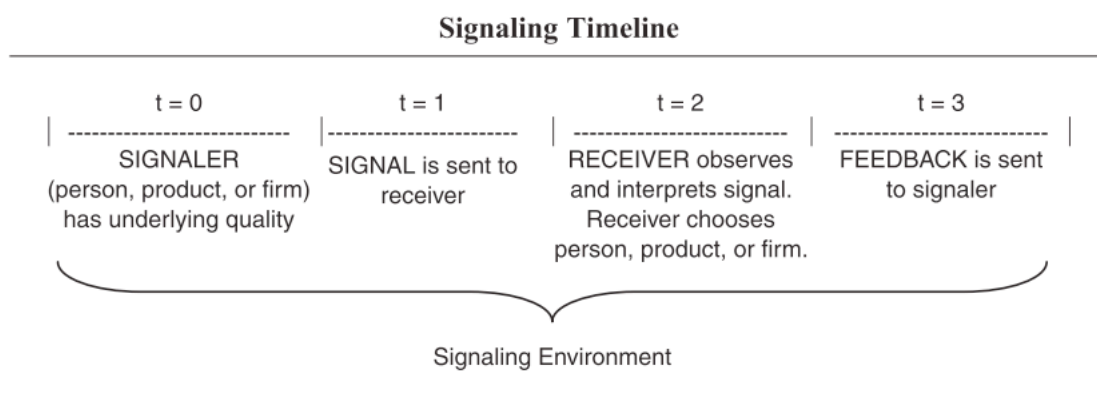
Michael Spence developed signalling theory in the context of asymmetric information of buyers and sellers that naturally exist within an economic market (Boulding & Kirmani, 1993) and social climate Connelly, Certo, Ireland & Reutzel (2011). Asymmetries are created when "different people know different things" (Connelly et al., 2011., p.42) and Spence defined signalling theory as "fundamentally concerned with reducing information asymmetry between two parties" (Connelly et al., 2011; Mavlanova et al., 2012; Wells, et

al., 2011).

Mavlanova et al. (2012, p.240) further described strategic signalling as “actions taken by a signaller to influence views and behaviours of receivers” (Mavlanova et al., 2012, p.240) based on the premise of previous literature which suggested that signalling theory’s underlying principle has been described as the use of a costly signal (i.e., must have cost the seller) sent for the signaller’s benefit (of anticipated revenue from the receiver), while the receiver uses the signal as a true reflection of the claims made by the retailer, otherwise the cost of the signal is not strategic (Connelly et al., 2011; Mavlanova et al., 2012).

Signalling theory has been used commonly by several disciplines for their examinations of behaviour surrounding information asymmetry. Connelly et al. (2011) researched the previous academic literature across multiple disciplines in order to provide a concise synthesis of the theory and its key concepts. In Figure 1 below, Connelly et al. (2011, p.43-44) created the frames of the “signalling environment” and identified that it includes two primary actors (at a minimum) – the signaller and the receiver – and then the signal itself.

Figure 1: Signalling Timeline (Connelly et al., 2011)



Note: t = time.

(Connelly et al., 2011) explained that, although there can be multiple signallers, signals and receivers, the literature previously focused on one-one or transaction-specific

communication. Connelley et al. (2011) included feedback ($t=3$ in the above figure) into the signalling environment, incorporating previous literature which had assumed that information asymmetry worked in two directions, where both signallers and receivers desire information and could therefore be, for example, a sender and receiver within the same exchange. For the purpose of this researches objectives transaction specific communication is focused on.

2.4.2 Signalling theory in the online marketing context

Signalling theory has been studied in the online marketing context, in light of the fact that asymmetries exist online and online sellers can control the information they provide to consumers when displaying their products, which they can easily manipulate, modify and change (Mavlanova et al., 2012; Wells et al., 2011). The intangibility of the online relationship has been found to increase the uncertainties that exist when making decisions. A basic example of signalling theory in the context of online commerce is product quality. Consumers cannot tangibly verify the quality of products they are purchasing and therefore rely on certain signals in deciding whether or not to purchase the product (Connelly et al., 2011).

Mavlanova et al. (2012, p.241) explained that the information asymmetry that exists between the company and consumers leads to two main problems for the online consumer, namely: (i) the ability of a company to misrepresent themselves to the buyer by distorting the seller's true characteristics before they contract and (ii) the "post-contractual" risk of non-fulfilment at the buyer's expense (e.g., non-delivery of a promise).

The former problem of misrepresentation can be resolved through the use of signals, while Mavlanova et al. (2012, p.241) suggested the second case could be resolved only by "incentive". Connelly et al. (2011) and Wells et al. (2011) also considered signalling theory to be effective when looking at different signals sent to the receiver before they purchase a product.

2.4.2.1 *Signals*

Academic literature identified that consumers use signals as symbols of information to aid

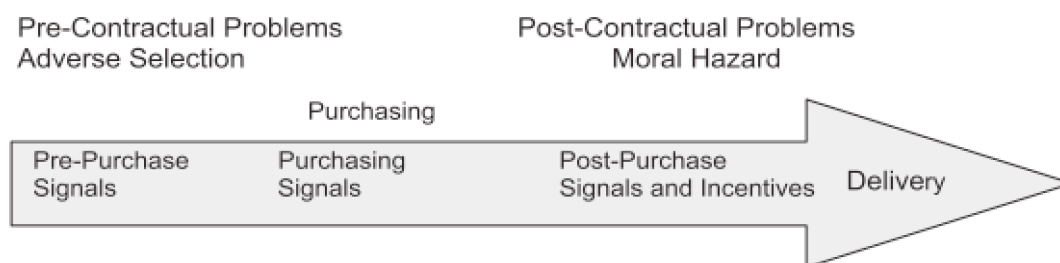
speedy evaluations and to infer the value of an online retailer or company, due to a signal or symbol being identifiable and easy to attain (Atkinson & Rosenthal, 2014; Mavlanova et al., 2012).

Kim & Kim (2011, p.148) discussed the common use of market signalling and proposed that the use of extrinsic signals, “such as money-back guarantees and privacy assurances”, are the most efficient in aiding the consumers’ ability to distinguish between the reliable and non-reliable retailers. Brand credibility, for example, was used as an extrinsic signal aimed at increasing brand consideration and trust due to the inferences consumers can easily make from the brand (Liberali et al., 2013; Kim & Kim, 2011; Aguirre et al., 2015).

2.4.2.2 Evaluating the properties of a third-party symbol as a signal within the signalling theory framework of Mavlanova et al. (2012)

Mavlanova et al. (2012, p.241) created a three-dimensional framework in which to evaluate the properties of website signals. This is discussed below in order to clarify signalling theory, and third-part signals are specifically referred to due to the research objectives. The purchase time continuum (Figure 2) forms the overarching frames or phases of the process with the three dimensions being time, ease of verification (Figure 3), and signalling cost (Figure 4).

Figure 2 The Purchase Time Continuum (Mavlanova et al., 2012)



In **Error! Reference source not found.**, a third-party seal would be a pre-purchase signal as it would influence the chance of “adverse selection” by the receiver, i.e. before any

action (purchase or request) is made. Purchasing and post-purchasing signals influence the fear of non-delivery and refer to signals that influence this risk or fear (Mavlanova et al., 2012, p.241).

Figure 3 : Characteristics of Signals (Mavlanova et al., 2012)

Characteristics of signals.

	Pre-contractual (adverse selection)		Post-contractual (moral hazard)			
	Pre-purchase		During purchase		Post-purchase	
	Easy-to-verify	Difficult-to-verify	Easy-to-verify	Difficult-to-verify	Easy-to-verify	Difficult-to-verify
Low cost	<ul style="list-style-type: none"> • Contact Information 	<ul style="list-style-type: none"> • Privacy Policy • Return Policy • Security Policy • Credit Card Logos 	<ul style="list-style-type: none"> • Secure Transaction (Secure Socket Layer Encryption) 	<ul style="list-style-type: none"> • Delivery Date Claim • In Stock Availability Claim • Product Quality Claim • Shipping Methods 	<ul style="list-style-type: none"> • Email Confirmation • <i>Coupons (promo codes as incentives to buy again)</i> 	<ul style="list-style-type: none"> • <i>Actual Delivery Date</i>
High cost	<ul style="list-style-type: none"> • Third-party Seals • Live Chat • Regulatory Compliance • Store Locator 	<ul style="list-style-type: none"> • Consumer Feedback • Domain Specific Content 	<ul style="list-style-type: none"> • Alternative Electronic Payment Mechanisms 	<ul style="list-style-type: none"> • Cash Back • Coupon Redemption 	<ul style="list-style-type: none"> • Order Status (tracking information) 	<ul style="list-style-type: none"> • <i>Actual Product Quality</i>

Note: Incentives are shown in italics.

Figure 4 Variables and Definitions of Signal (Mavlanova et al., 2012)

Variables and definitions.

Signaling cost		Ease of verification	
High cost signals	Low cost signals	Difficult to verify signals	Easy to verify signals
Third Party Seals	Contact details	Credit card logos	Contact details
Domain Specific Seals	Credit card logos	Privacy Policy	Third Party Seals
Live Chat	Privacy Policy	Security Policy	Domain Specific Seals
Store Locator	Security Policy	Return Policy	Live Chat
Prescription Requirements	Return Policy	HIPAA privacy policy	Store Locator
Consumer Feedback	HIPAA privacy policy	Consumer Feedback	Prescription Requirements
Electronic Payments	Secure Transactions	Health Content	Secure Transactions
Health Content			Electronic Payments

Note: Only signals that appear in pre-purchase and purchasing phases are listed.

As per Figures 3 and 4, a third-party seal, was identified as a high-cost, easy-to-verify signal at the pre-contractual phase of the framework. They are of high value as they can only be received from an independent certifying body, and authorising industry standards are being upheld; they require actual payment for membership; and they can be authenticated on the independent certifying body's website (Mavlanova et al., 2012; Wells et al., 2011).

2.4.3 Third-party seals, signalling theory and privacy concerns

While online consumers have relied on signals to identify qualities of a retailer, companies and retailers online have been known to use these same signals deceitfully in attempting to increase consumers' trust and mitigate their online privacy concerns (Kim & Kim, 2011). Online consumers can, therefore, be at a disadvantage, as they have to rely on what the company says or displays they are doing as being true. When looking at this deception, and reliance of the consumers on retailer information in light of consumers' privacy concerns, consumers are having to believe what a company and retailer is saying they are doing with the consumers private information (i.e. in their terms and conditions). The lack of control for consumers will spark their vulnerability and concern surrounding the information management. In academic research and literature, signalling theory has helped to identify ways for companies to reduce the feeling of risk for consumers within the online asymmetry, which resulted in consumers being more responsive towards disclosing information of a private nature (Liberali et al., 2013 p.103).

In disclosing private information online, it is therefore imperative that the company creates an environment where the consumer can easily and readily identify when their information is at risk and when it is not, in order for the consumer to make a rational decision whether or not to engage with the company (John et al., 2011; Pavlou, 2011).

Kim & Kim (2011) recommended that companies should take the initiative to inform consumers about their online data privacy practices, as this acts as a signal that the company is trustworthy. The presence of a third-party seal has been found to have a positive effect on the perception of trust for a website, both in academic literature and by advertising bureaus (Aguirre et al., 2015; Kim & Kim, 2011; Smith et al., 2011; Xu et al., 2011). Studies have suggested the use of signals within companies' advertisements to counter the negative impacts of information asymmetry when customers are purchasing online (Acquisti et al., 2012; Aguirre et al., 2015; Kim & Kim, 2011). Aguirre et al. (2015) found that within the context of companies' collections of personal information on social media, advertisements that incorporated personalisation and third-party privacy symbols increased the consumer trust in the brand. Smith et al. (2011) pointed out that research on third-party seals identified them as effective signals and a beneficial effect on a consumer's trust in a website.

2.5 Consumer Disclosure of Private Information

2.5.1 The private nature of disclosing income

Consumers commonly identify personal or household income as a highly private piece of information. In Goldfarb & Tucker (2011, p.28) they identified that “people who refuse to answer questions on income usually do so because of concerns about privacy”. Legal and company privacy policies tend to specify that health and financial products be considered as private information. These are also identified in academic literature as sensitive information for consumers, the privacy of which is particularly important (Tsai et al., 2011).

Goldfarb & Tucker (2011, p.349) identified a common consumer concern towards answering questions about personal financial information and that consumers were much more prone to protect this information than disclose it – and observed in several studies that people who refuse to answer questions on income usually do so because of their privacy concerns (Goldfarb & Tucker, 2011; Goldfarb & Tucker, 2012; Tucker, 2012).

Goldfarb & Tucker (2012) used a popular database in order to study changes in how consumers disclosed their private information over time. The database is commonly used within the online media industry, and has been used in previous academic literature as a benchmark for advertisement design (Goldfarb & Tucker, 2012, p.350). In their study, Goldfarb & Tucker (2012, p.350) found that the refusal by consumers to disclose their information on income was “15% (percent) on average”, where refusal to disclose other types of private information was “less than 0.5%”.

More recently, Leon, P. G., Rao, A., Schaub, F., Marsh, A., Cranor, L. F. & Sadeh, N. (2015, p.5) confirmed that participants in their study were not comfortable revealing information around their income bracket, credit score and sexual orientation and identified them as private, “nobody’s business” information. The consumers stated further that they experienced the mere collection of such information to be a direct “invasion of their privacy” (Leon et al., 2015, p.5). Income is, therefore, used as a dependent variable in the study as it helps to identify that the consumer has effectively disclosed what is commonly

believed to be private information.

Mothersbaugh et al. (2012) saw similar results in creating their higher sensitivity index for their disclosure study. They performed a pre-test on their data, whereby they identified the information that caused their respondents the most discomfort and risk in their willingness to disclose information. The data revealed that banking and income information were of a highly sensitive nature. They used these factors in their index as highest value in their further testing of disclosure.

2.5.2 Do different demographics disclose private information differently?

Smith et al. (2011, p 1002) identified that in previous literature, different demographic group reactions to disclosure of private information (between, for example, “gender, race, income and culture”) were compared (Xu et al., 2012, p.10). They looked at previous research where demographic differences (specifically around gender and education level) influenced the degree of privacy concerns for an individual, and controlled for this influence in their analysis of their research “because they could potentially affect the degree of privacy concerns in a specific context”.

Atkinson and Rosenthal (2014) studied whether demographics still influenced the degree of privacy concerns and disclosure amongst their data subjects and concluded that a significant difference existed with respect to age, gender and income.

The demographics of age, gender and income brackets are, therefore, discussed below in context of the relevant academic literature to identify their relevance in the current research objectives.

2.5.2.1 *Age*

Several studies have identified that disclosure and behaviour around privacy concerns are different across age groups (Acquisti et al., 2012; Goldfarb & Tucker, 2011; Mothersbaugh et al., 2012). Goldfarb & Tucker (2012, p. 349) found that behavioural differences in privacy-protective behaviours could be seen across age. They specifically noted that older generations are more averse to revealing personal information than the younger

generations, due to the nature of older people being particularly private in personal contexts. Mothersbaugh et al. (2012, p.9) included age as a co-variate in their research due to industry evidence by the Pew Internet and American Life Project (2009), that “age is a major demographic factor influencing Internet use and purchase”.

Kim used a sample of students for their online shopping research, as they had noted from the previous literature that they would get more information from this sample because of the expected lower privacy concerns in younger generations, and therefore the higher likelihood to purchase online.

It is therefore important to identify whether there is a difference between various age groups in the context of disclosing personal information online for the purpose of a service.

2.5.2.2 *Gender*

Acquisti et al. (2012, p.35) found significant gender differences between how men and women reacted and responded to personal questions. They also found that men were much more consistent among themselves in their general response, but women differed quite substantially between them in their responses. Jansen, Moore and Carman (2013) discussed that – although it may be seen as a generalisation – previous research had identified a clear difference in the way men and women process certain information, specifically surrounding stimuli such as schema and images versus text. However, in the online context, differences have not been as clearly visible whereby several studies revealed different findings, including some with very insignificant differences. Jansen et al. (2013, p.289) assumed the narrowing of gender difference could be explained due to the reality “Internet has become more integrated into people’s daily lives”. The Goodrich (2014, p.33) study found that males rely more heavily on schema and heuristics to make decisions than females do and further noticed that mere exposure “works” better with males than females with regard to online advertising.

It is, therefore, important to identify whether this gender difference does exist within the context of disclosing personal information for the purpose of a service.

2.5.2.3 *Computer and mobile*

Özpolat and Jank (2015, p.55) suggested that, with the growth of mobile connectivity and widespread use of the Internet, the trust formation process among consumers should replicate previous studies including more mobile data. Ström, Vendel and Bredican (2014, p.1007) noted computer users as more frequently using the Internet than mobile users because the input of data was easier due to the screen size.

Situations that differentially activate privacy concerns will lead to different levels of disclosure, even if they are equivalent with respect to the objective costs and benefits of disclosure cues. John et al. (2011, p.368) identified that signal decreases in “objective dangers of disclosure (examples include receiving spam e-mails as a result of divulging one’s e-mail address and having one’s identity “uplifted” as a result) can lead people to be less forthcoming with information: individuals given assurances of confidentiality are more willing to complete a questionnaire than those receiving no assurance”.

Research teams from the search engine Google compared the differences between usage of computer and mobile device consumers and noticed various differences in consumers search behaviour between desktop users and mobile device users (Westlund, Gómez-Barroso, Compañó & Feijóo, 2011, p.694).

Keith, Thompson, Hale, Lowry and Greer (2013, p.1172) examined location-based mobile applications and consumer disclosure and found that, in contrast to prior research on privacy disclosure (on websites as opposed to mobiles), perceived privacy risks played a larger role than perceived benefits in determining disclosure intentions on mobile than on a desktop.

CHAPTER 3

3 RESEARCH HYPOTHESES

3.1 Introduction

The broad objective of the study was to examine empirically whether a third-party privacy seal (lock) contained in an e-mail advertisement could aid a company in mitigating consumer privacy concerns, acting as a high-quality signal to the consumer, through a live experimental test whereby a control group (Group B) would receive an e-mail without a third party seal, and an experimental group (Group A) would be sent an e-mail advertisement with a third-party privacy seal (lock).

3.2 Hypotheses

From the literature review, four main hypotheses were established:

3.2.1 Hypothesis 1

Group A will have a higher conversion rate (i.e., more consumers will disclose income) than group B, due to the image of the privacy seal / lock on the e-mail advertisement.

The objective here is to identify whether a third-party privacy seal (lock) is enough of a high-value signal for consumers that they will disclose personal information because of it.

$H_0\#1$: There will be no difference in disclosing income between Group A and Group B across all the databases.

$H_A\#1$: There will be a difference between Group A and Group B in disclosing their income across all the databases.

3.2.2 Hypothesis 2:

Group A will have a higher click-through rate (i.e., more consumers will click on the e-mail links) than group B, due to the image of the privacy seal / lock on the e-mail advertisement. This objective responds to the Mothersbaugh et al. (2012) suggestion for further research in different contexts by using the click-through test on an e-mail advertisement, identified in literature as mistrusted and linked to consumer privacy risks due to their common identification as spam (Kim & Kim, 2011).

$H_0\#2$: There will be no difference in Click-through between Group A and Group B across all the databases.

$H_A\#2$: There will be a difference in Click-through between Group A and Group B across all the databases.

3.2.3 Hypothesis 3:

Consumers will be more likely to convert (i.e., disclose their income), when accessing the website via a desktop or laptop computer than when accessing the website via a tablet and a mobile device (device category), due to the privacy concerns activated via mobile phones.

Özpolat and Jank (2015, p.55) suggested that, due to the rapid growth of mobile connectivity, previous studies, relating to the trust formation process among consumers should be replicated; in order to explore and understand the impacts of mobile devices on previously explored topics.

$H_0\#3$: The device (mobile, desktop or tablet) being used will not make a difference to disclosure of personal information (lead).

$H_A\#3$: The device (mobile, desktop or tablet) being used will make a difference to the disclosure of personal information (lead).

3.2.4 Hypothesis 4:

Jansen et al. (2013) identified that while traditionally responses between genders were

significantly different, this significant difference is not so evident within the online context. Base J already had this data and therefore it could be explored further.

$H_0\#4$: There will be a difference between the genders response rates in Group A and Group B.

$H_A\#4$: There will be no difference between the genders response rates. In Group A and Group B.

CHAPTER 4

4 RESEARCH METHODOLOGY

4.1 Introduction

The principle of Causal Theory stems from the law of cause and effect, which allows researchers to propose theories that are testable (Saunders & Lewis, 2012, p.105). Causal research seeks to measure (independent) variables that explain the reaction of a dependent variable (Saunders & Lewis, 2012, p.105). Experimental designs are the most rigorous, powerful and the strongest of the design categories to establish a cause-effect relationship (Lavrakas, 2008, p.728).

Saunders and Lewis (2012, p.114) proposed that the essential components (i.e., conditions) of an experiment are:

1. Manipulating independent variable/s;
2. Controlling the experiment holding all but the dependent variable constant;
3. Observing the effect of the manipulation of the independent variable on the dependent variable;
4. Predicting events that will occur in the experimental setting.

4.2 Research Design

Holding detailed consumer information is a company's competitive advantage in today's data-driven world; and Internet marketing is a major source of trackable and verifiable revenue for companies worldwide. With high marketing budgets being spent on Internet marketing, a return on such investment needs to be evident and visible for stakeholders.

This research aimed to show such a cause-and-effect relationship of a trust symbol in an e-mail advertisement on the privacy concerns and trust of a consumer by examining the disclosure of private information by the data subject (consumer) on a website form. Since the problem was well defined, this research sought to establish evidence of a causal

relationship through the treatment conditions of a true experimental research design (Lavrakas, 2008). Lavrakas (2008) described the experimental process as follows:

1. The researcher deliberately manipulates one or more independent variable/s (trust symbol);
2. Randomly assigns individuals or objects to the experimental conditions;
3. Measures the effect of the independent variable (third-party privacy seal) on one or more dependent variable/s (yielding income information on a web form);
4. Controls other environmental and extraneous variables.

This research aimed to meet the first three conditions. The final condition cannot be met in its entirety, as not all extraneous variables, whether identified or not, can be controlled.

The research method was chosen to examine the hypotheses and research objective; it consisted of a live experimental randomised two-group post-test design (Lavrakas, 2008, p.726). The experiment was conducted through a randomised field experiment called an A/B split test, where one group (*Group A*) is sent an e-mail advertisement with an image of a lock on it, and another group of data subjects (*Group B*) is sent an e-mail advertisement without an image of a lock.

This design was chosen as the best and simplest design to use for the purposes of testing the research hypotheses for the following reasons:

- It involves two groups; a control group (B) and an experimental group (A);
- Group members were randomly selected from the population and randomly (R) assigned to the experimental or control groups;
- The effects of the experimental treatment on the dependent variable are measured at the conclusion of the experiment (O). This is known as the post-test observation.

Lavrakas (2008) clarified that this type of experiment is expressed as Experimental Group: *R A O* and Control Group: *R B O*. The two-group post-test design (A/B test) allowed the researcher to develop causality and examine the seal's interaction with other variables.

Three databases from a single South African company, within the online lead generation

industry, were used and consolidated for the purposes of the test. The databases used were from three separate “white-label” brands all owned by the company (*Base H, Base Y, Base J*), which offers a “middle-man” service connecting financial services partners with consumers looking for products. They do this through multiple advertising channels such as e-mail advertisements, Google adwords and search engine optimisation, white label marketing, social media platforms, mobile advertising, affiliate marketing. They use several brands to advertise through, which gives them a bigger share of the market, offering consumers comparable financial service product quotes from several insurance providers. The company further cross-market products and service to consumers who have previously used their online services.

An electronic mail advertisement (e-mail advertisement) was used to perform the test as e-mail advertisements were identified in the literature as cues that signal to consumers that an “objective danger” exists – for example “receiving spam e-mails as a result of divulging one’s e-mail address and having one’s identity ‘uplifted’ as a result”. The “objective danger” has been shown to result in consumers being more averse to disclosing their private information. Adding privacy assurances such as third-party privacy seals can combat this aversion (John et al., 2011). The type of third-party privacy seal used (lock) was based on previous research, which identified positive effects of the trust symbol when used on a website (Aguirre et al., 2015), as well as the icons the seal providers recommended. In order to use the icon, the company has to be registered with the seal provider.

4.2.1 Validity of the research

The research is valid in both its internal and external facets, but several limitations were identified in the limitations paragraphs below. Saunders and Lewis (2012, p.127) refer to several factors that threaten the internal validity of research, including subject selection, testing, mortality and ambiguity about causal direction. Causal direction ideally shows the flow effect of the independent variable on dependent variables (Saunders & Lewis, 2012).

Extraneous variables affect this flow and threaten internal validity. Such variables include: (i) history, such as previous brand experience and pre-conceived notions of privacy and trust online; and (ii) mortality or the loss of a data subject during the research (Saunders &

Lewis, 2012). In this context, it refers to subjects being disconnected, while still browsing the website because of connectivity issues as well as ISP or deliverability issues of electronic mails. This should, however, affect all subsets of the data. Saunders and Lewis (2012, p.128) explained that external validity refers to whether the cause-and-effect relationship found in the research can be generalisable to other research settings.

Internally, the data groups are equivalent to each other as they are assigned randomly from the same population of data subjects. Each database was split into two groups Group A (lock) and Group B (No lock). In total 6 (six) e-mail advertisements were sent out over a one-month period. These data subjects were analogous with regard to the following aspects:

- All the participating consumers are South Africans over 18 years of age
- All had subscribed to the database voluntarily, which allows the company to use the private information that the consumers provided to the company. All the participating consumers use the Internet to subscribe to these services as the company is solely based on the Internet
- The data subjects disclosed various types of private information to the company, such as name, surname and e-mail address, but have not previously disclosed income voluntarily.

4.3 Universe

The sample population consisted of the database of consumers from a single South African company. The data subjects are all online consumers. The universe consisted of consumers from Group A and Group B who click on the e-mail advertisement; and the consumers from Group A and Group B who disclose their income (private information) on the website form.

All elements on the e-mail advertisements were kept the same to allow testing of whether adding a third-party privacy seal (lock) had an impact on the consumers' behaviour. The third-party privacy seal (lock) formed part of the visual design of the campaign and was the only differentiating variable on the two e-mail advertisements that were sent to Group A and Group B. The subject line was kept the same so as not to influence the open-rate

percentage of the e-mail advertisements. The subject line was “*Hospital plan or medical aid?*”

Figure 5 Lock – Group A – e-mail advertisement

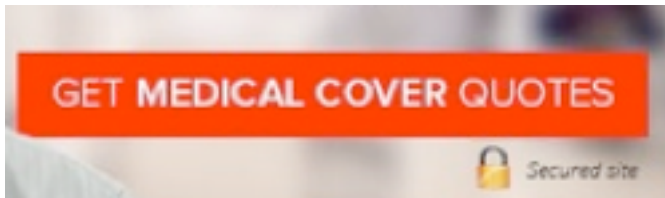
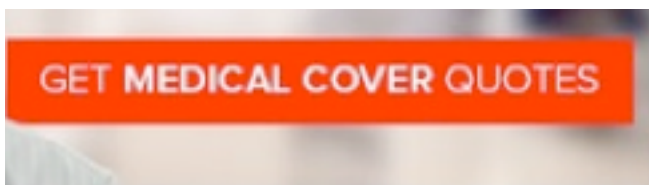


Figure 6 No Lock – Group B –e-mail advertisement



4.4 Sampling Method and Size

Only a sample of the population was used. The e-mail advertisement was sent to a sample of the consumers belonging to the company’s complete database list (population) (Saunders & Lewis 2012). Random probability sampling was used as consumers were selected randomly from the company’s database for the purpose of testing the hypotheses (Saunders & Lewis 2012). An e-mail advertisement could not be sent to the entire population as its providers limited the company as to how many consumers could be sent to their providers at one time. Due to the experiment being done in real-time, it was important that consumers were satisfied with delivery of the service and experienced the real-life experience to ensure that the experiment is not compromised by external factors.

A random convenience sample of 267 612 data subjects was used for the experiment due to the company’s previous experience of how many consumers would respond to the data. The sample size used was based on previous external limiting factors identified by the company in obtaining a robust sample size that would be significant enough to

analyse whether a causal relationship existed.

Identified external effects include a lack of response as the company had assumed a maximum 10% of the data subjects opening the e-mail advertisement and 2% of the data subjects clicking on the e-mail advertisement due to the product being advertised (medical insurance) as well as the type of database being used.

The test was staggered across a 30-day period so as not to inundate the financial service partners (providers).

133 804 e-mail advertisements were sent to Group B and 133 808 e-mail advertisements were sent to Group A. They were, however, sent over three 'sends' and while they were initially consolidated into one concise base, they were then split by brand. (*Base X, Base Y, Base Z*), The list was randomised into a Group A and Group B through the following process:

1. All three brands (*Base X, Base Y, Base Z*) used the sample of their population that had been collected over the past year (12-month) period for financial services. This period was chosen due to legislation of the Protection of Personal Information Act 2012, which stated that you can only use private information you have collected, within a reasonable time period, and the company has identified 'reasonable' to be one year (12 months).
2. Both Group A and Group B were sent an e-mail advertisement each for a financial services product, namely medical aid. This product was chosen due to the income field being on the form where the data personal information was requested.
 - a. The experimental group (Group A) was sent an e-mail advertisement with a trust symbol placed on the advertisement. Appendix A contains an example image of Group A's e-mail advertisement. The control group (Group B) was sent an e-mail advertisement without a trust symbol on it. Appendix B contains an example image of Group A's e-mail advertisement. The e-mail advertisements 'sends' were staggered over the 30-day period. Each send sent out the same number of e-mail advertisements to Group A and Group

B so as to mitigate external variables influencing the experiment.

3. If a consumer (data subject) clicked on the e-mail advertisement, they landed on the same website irrespective of which group they belonged to. Appendix C shows an example image of the website that the Groups landed on. Appendix C white label website, which advertised quotes for medical cover and contained the third-party privacy seal (lock) as per the SSL providers' requirements. The website had a form on it where the data subjects could disclose their private information should they wish to be contacted by providers and receive comparable quotes. The private information requested consisted of name, surname, e-mail, contact number and income bracket.

4.5 Unit of Analysis

In order to answer the hypothesis, the unit of analysis for the research was the individual consumer's (data subjects) response.

4.6 Data Gathering

"Quantitative marketing research addresses research objectives through empirical assessments that involve numerical measurement and statistical analysis" (Zikmund & Babin, 2012, p.99). The data gathered was quantitative and of a nominal nature because a consumer either clicked on the e-mail advertisement or did not click, and a consumer either disclosed their income or did not. The data used was gathered by tracking the behaviour of consumers who received the e-mail advertisements and disclosed their information on the website form. Zikmund and Babin (2012, p.191) identified this setting as observational in nature as the data was gathered in an experimental setting.

The data was gathered and tracked, using the company's internal e-mail system (the system), which tracks and measures each consumer through the nominal data. The system gave the following nominal data: whether or not a consumer opened their e-mail advertisement (*opens*); as well as the percentage of overall consumers who opened the e-mail advertisements among all the consumers who received the e-mail (*open-rate*); whether or not a consumer clicked on the e-mail advertisement (*click-through*); and

whether or not a consumer disclosed their income (*conversion*).

The data gathered was also tracked on Google Analytics, an external tracking tool that uses the nominal data to help companies to measure. Google analytics (GA) allows you to select any subset of data and look at its patterns over customer (user) activity such as where do visitors come from, and certain demographics (age, gender) as well as the device a user is accessing the website from (i.e. mobile or web) (Manovich, 2011). A google analytics (GA) client (i.e. the company) has the ability to export data into Microsoft Excel format which can be used to further analyse and trend the data on graphs and charts (Plaza, 2011). In order to track the subset of data via GA, a measurement tag provided by GA, needs to be placed on the website which allows Google to then track the specific data. Google Analytics (GA) was used in examining Hypothesis 2 and Hypothesis 3 for the results, and was used further in the discussion section for Hypothesis 3 and 4. The Google Analytics (GA) measurement tag was placed on the relevant pages on the website to track the e-mail advertisements. The period over which the e-mail was sent across all three sends was selected, 1 August 2015 to 1 October 2015, for analysis.

The internal systems used by the company and, as well as GA, are both Internet-based interfaces that translated into CSV files that were downloaded, merged and analysed.

4.7 Data Analysis

The IBM software SPSS allowed the researcher to set the parameters for statistical research. For the purposes of hypothesis 1, 2 and 4 this included the chi-square two-table test, with statistical significance at a 95% confidence interval. The purpose of this work was to analyse the probability of an association between two variables” as recommended by Aguirre et al. (2015, p.40) and Saunders and Lewis (2012, p.180). The data is with more than one variable, and therefore two-way tables are used for the analysis in order to provide a foundation for statistical inference in the results of the two groups and associations involved.

For hypothesis 3 a factorial analysis of variants was used, as the data analysed is variable data in the form of continuous measurement. Descriptive statistics were used to interpret the results with a focus on the difference between the means (LS means) of the variants.

The Games-Howell post hoc test was used to see where the differences between variants existed because the variances were different across device categories and this test takes difference in variance into account.

4.8 Limitations

The research had a variety of limitations. Some were identified before the experiment was embarked upon, but a lot of them revealed themselves throughout the experimental and analysis process and have been used as recommendations in the conclusion of the research.

Initially, the limitations were the following:

- The population sample consisted of South African consumers. The experiment was limited to South African providers and therefore does not take into account cultural and global differences. It was limited to financial services and while this is specific to the context, it may be generalised globally through this product
- The size of the data limited the robustness and significance of the data, due to low response rates
- The consumers had previously disclosed private information to the company and therefore may have already been less risk-averse than other consumers to disclosing income
- The observational nature of the experiment was also a limitation because it did not gather any qualitative data that may have contributed to the consumer's (data subject) behaviour such as attitudes, motivations and preferences (Zikmund & Babin, 2012, p.191).
- The e-mail advertisement that was used, advertised financial services products, and therefore Base H and Base Y already had an affinity to these products. Consumers were not asked if they had previously wanted the product being advertised to them and it is limitation to the study that we can base the findings on the experimental data only.

There were several further limitations that resulted from the way the company stored its databases and gathered its information. The limitations were created due to the following

practices (storage and systems) of the company:

- The company stored its brand databases separately and each brand collected different types of information from its consumers. Some, for example, stored age and gender, where others stored province and city. Base J had a database with gender (due to the information collected on a person joining the entertainment portal) and this was used for Hypothesis 4.
- The company did not store information it had collected covertly in a way that could be utilised for each individual consumer, but rather stored it in a format that anonymised the data as per the POPI act regulations.
- Mobile statistics were not analysed for the specific data subjects before the test and Google Analytics were the only statistics cold be used for post-test analysis.

CHAPTER 5

5 RESULTS

The results from the research will be presented in this chapter. The objective of this research was to explore if there is a causal relationship between a third-party privacy seal (lock) used as a signal in an e-mail advertisement and consumer behaviour on the internet by examining the effect on disclosure of personal information generally and between genders, clicks on an email generally and between genders and the disclosure of personal information on different devices (desktop, mobile and tablet).

The results will be presented in two sections. Firstly descriptive statistics will be discussed followed by the inferential statistics. For the inferential statistics section results will be relating to each hypothesis, with reference to the types of statistical tests run as well as the statistical interpretation of the results received. This section will include additional inferential statistics related to the results. The chapter will conclude with a summary of the results leading into a deeper discussion through Chapter 6.

5.1 Descriptive Data

Table 1 Descriptive Data of sample

Total Database		
Sent	Clicked	Disclosed Information
267612	1632	134

A total of 267,612 e-mail advertisements were sent to three database of one South African company (Brand H, Brand J and Brand Y). Group A was sent 133,808 e-mail advertisements containing the third-party privacy seal (lock) and Group B was sent 133,804 e-mail advertisements without the third-party seal (no-lock). In total 1632 of the

data subjects, being 0,61% of the base responded to the e-mail advertisement by clicking on it. 134 data subjects disclosed their income, being 0,0501% of the total base and 8,21% of the respondents.

5.2 Inferential statistics for each hypothesis

5.2.1 Hypothesis 1

This section examines whether the third-party privacy seal (lock) impacted consumer disclosure. Of all the recipients of the e-mail advertisement across both Group A (Lock) and Group B (No Lock), only 134 participants disclosed their personal information (income). 65 of these were from Group B and 69 were from Group A. The statistical significance and results are discussed below through the chi-square test that was used to analyse the categorical data. Table 1 looks at the results for hypothesis 1.

5.2.1.1 Hypothesis 1 Results

Table 2 Hypothesis chi-square two-way test and summary table of observed frequencies across all data subjects

Marked cells have counts > 10. Chi-square (df=1)=0.12, p=0.72973			
Third Party Seal	Disclose Income NO	Disclose Income YES	Row Totals
No Lock	133739	65	133804
Row %	99.95%	0.05%	
Lock	133739	69	133808
Row %	99.95%	0.05%	
Totals	267478	134	267612

The Null hypothesis, that there will be no difference in disclosure between Group A and Group B, is accepted across the bases. This is accepted due to no significant difference

existing between the results, as indicated by the p value in table 2 being greater than 0.05%. (P value is 0.72973), using a confidence interval of 95%. This therefore signifies that there is no association between the third-party privacy seals (lock) and clicks across the data subjects.

5.2.1.2 Results per Brand for disclosure of income

Table 3-5 below are based on the chi-square two table test we ran on each brand separately, in order to analyse their individual impacts. Although these are not hypothesized they were tested for analysis and discussion purposes. We discuss each brand results in the paragraphs below:

BASE J

Table 3 chi-square two-way test and summary table of observed frequencies for Base J

Marked cells have counts > 10. Chi-square (df=1)=0.73, p=0.39241			
Lock/No Lock	Disclose Income NO	Disclose Income YES	Row Totals
No Lock	65522	13	65535
Row %	99.98%	0.02%	
Lock	65526	9	65535
Row %	99.99%	0.01%	
Totals	131048	22	131070

131,070 e-mail advertisements were sent to Base J being the largest database used for the test. Across both Group A (Lock) and Group B (No Lock), only 22 participants disclosed their personal information (income). 13 of these were from Group B and 9 were from Group A. The p value in table 2 being greater than 0.05%. (P value is 0.39241) shows that this minor difference was not significant and/or there was no association for either group.

BASE H

Table 4 chi-square two-way test and summary table of observed frequencies for Base H

Marked cells have counts > 10. Chi-square (df=1)=2.50, p=0.11369			
Lock/No Lock	Disclose Income NO	Disclose Income YES	Row Totals
No Lock	35376	23	35399
Row %	99.94%	0.06%	
Lock	35366	35	35401
Row %	99.90%	0.10%	
Totals	70742	58	70800

70,800 e-mail advertisements were sent to Base H. Across both Group A (Lock) and Group B (No Lock), only 58 participants disclosed their personal information (income). 23 of these were from Group B and 35 were from Group A.

The Null hypothesis, that there will be no difference in disclosure between Group A (Lock) and Group B (No lock), is accepted for base H. The p value in table again is greater than 0.05%. (P value is 0.11369), shows that this minor difference was not significant and/or there was no association for either group.

BASE Y

Table 5 chi-square two-way test and summary table of observed frequencies for Base Y

Marked cells have counts > 10. Chi-square (df=1)=0.30, p=0.58573			
Lock/No Lock	Disclose Income NO	Disclose Income YES	Row Totals

No Lock	32841	29	32870
Row %	99.91%	0.09%	
Lock	32847	25	32872
Row %	99.92%	0.08%	
Totals	65688	54	65742

65,742 e-mail advertisements were sent to Base Y. Across both Group A (Lock) and Group B (No Lock), only 54 participants disclosed their personal information (income). 29 of these were from Group B and 25 were from Group A. Again for Base Y due to the p value being greater than 0.05%. (P value is 0.58573), using a confidence interval of 95%, this minor difference was not significant and/or there was no association for either group.

5.2.2 Hypothesis 2

This section examines whether the third-party privacy seal (lock) impacted click-through rates. Over all three databases in both Group A (Lock) and Group B (No Lock) only 1632 people clicked on the link. 518 of these were from Group B and 1114 were from Group A. The statistical significance and results are discussed below through the chi-square test that was used to analyse the data. Table 6 represents hypothesis 2 results from the chi-square test.

5.2.2.1 Hypothesis 2 Results

Table 6 Hypothesis 2 chi-square two-way test and summary table of observed frequencies across the data subjects

Marked cells have counts > 10. Chi-square (df=1)=224.09, p=0.0000			
Lock/No Lock	Clicked NO	Clicked YES	Row Totals
No Lock	133286	518	133804

Row %	99.61%	0.39%	
Lock	132694	1114	133808
Row %	99.17%	0.83%	
Totals	265980	1632	267612

Here the null hypothesis, that there is no difference in clicks between Group A and Group B is rejected as the P value is 0 which is below 0.05% and therefore the getting the data set on the assumption that null hypothesis is true is too low using a confidence interval of 95%. This means the alternate hypothesis that there is a difference between Group A (lock) and Group B (No lock) due to the third-party privacy seal (lock) is accepted. This therefore represents that there is an association between the third-party privacy seals (lock) and clicks across the data subjects.

5.2.2.2 Results per Brand for disclosure of income

Table 7-9 speaks to each individual base. The reason these are discussed separately is due to the different brands belonging to JHY that were used and analysed individually. Although not hypothesised these are relevant for both the results and discussions.

BASE J

Table 7 chi-square two-way test and summary table of observed frequencies for Base J

Lock/No Lock	Marked cells have counts > 10. Chi-square (df=1)=407.01, p=0.0000		
	Clicked NO	Clicked YES	Row Totals
No Lock	65284	251	65535
Row %	99.62%	0.38%	
Lock	64618	917	65535
Row %	98.60%	1.40%	

Totals	129902	1168	131070
--------	--------	------	--------

Base J sent the highest number of e-mail advertisements, 131,070. Across both Group A (Lock) and Group B (No Lock), only 1168 participants clicked on the e-mail advertisement, 251 of these were from Group B and 917 were from Group A, showing a higher click rate for Group A. The P value was below 0.05% ($p=0.0001$) and therefore the probability of difference between the number clicks in Group A and Group B is significant, representing an association between the third-party privacy seals (lock) and clicks for Base J.

BASE H

Table 8 chi-square two-way test and summary table of observed frequencies for Base H

Marked cells have counts > 10. Chi-square (df=1)=1.30, p=0.25457			
Lock/No Lock	Clicked NO	Clicked YES	Row Totals
No Lock	35234	165	35399
Row %	99.53%	0.47%	
Lock	35256	145	35401
Row %	99.59%	0.41%	
Totals	70490	310	70800

For Base H the P value is above 0.05% (P value is 0.25457 and the difference between the groups is therefore insignificant. Base H sent 70,800 e-mail advertisements and while 310 data subjects clicked on the e-mail advertisement (a higher percentage than both Base J and Base Y), 165 of these were from Group B and 145 were from Group A and the p value shows no association between the third-party privacy seals (lock) and clicks for Base H.

BASE Y

Table 9 chi-square two-way test and summary table of observed frequencies for Base Y

Marked cells have counts > 10. Chi-square (df=1)=16.57, p=0.00005			
Lock/No Lock	Clicked NO	Clicked YES	Row Totals
No Lock	32768	102	32870
Row %	99.69%	0.31%	
Lock	32820	52	32872
Row %	99.84%	0.16%	
Totals	65588	154	65742

Base Y sent 65,742 e-mail advertisements. Only 164 data subjects clicked on the e-mail advertisement, 102 of these were from Group B and 52 were from Group A

For Base Y the P value below 0.05% and therefore the probability of difference between the number clicks in Group A (lock) and Group B (no lock) is significant, representing an association between the third-party privacy seals (lock) and clicks for Base J. The difference in the significance/ association between Base J and Base Y is that there was a higher click rate for Group B (no lock) as opposed to Base J which showed a higher click rate in Group A (lock).

5.2.3 Hypothesis 3

This section examines whether a difference in a consumer's disclosure of personal information (lead) exists when on a mobile, desktop or tablet device.

For the testing of this hypothesis a Factorial analysis of variance was used. This differed from the other three hypothesis tests as the data was a continuous measurement and not categorical.

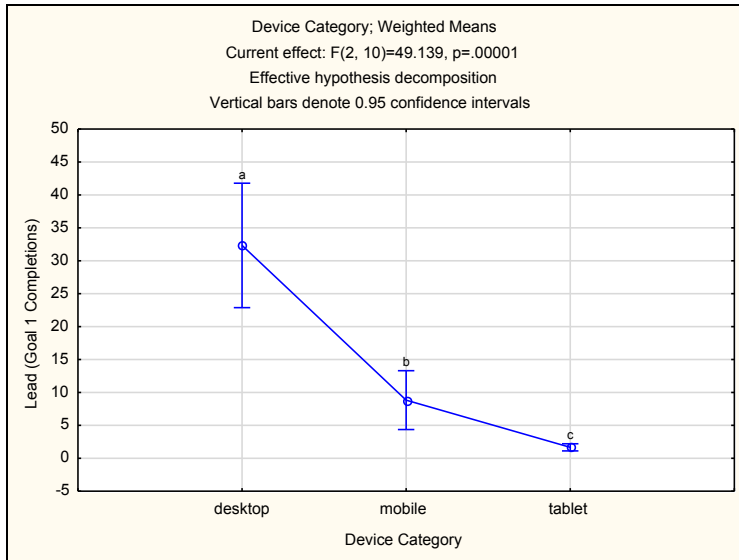
Table 10 below (Univariate Tests of Significance) describes the interaction effect of the third-party privacy seal (lock) across devices was not different. This was assessed before analysing the rest of the data. The null hypothesis is that the differences between the devices is the same for the lock and no lock, and this hypothesis is accepted due to the p value being 0.92 which is greater than the 95% confidence interval.

Table 10 Univariate tests of significance for lead (disclosure of personal information)

Effect	Univariate Tests of Significance for Lead (Goal 1 Completions) (Spreads Sigma-restricted parameterization Effective hypothesis decomposition; Std. Error of Estimate: 5.6056)				
	SS	Degr. of Freedom	MS	F	p
Intercept	3669.389	1	3669.389	116.78	0.00
Brand	168.444	2	84.222	2.68	0.12
Lock/No lock	9.389	1	9.389	0.30	0.60
Device Category	3088.111	2	1544.056	49.14	0.00
Lock/No lock*Device Category	5.444	2	2.722	0.09	0.92
Error	314.222	10	31.422		

Once concluding the interaction effects, the mean difference on the three effects can be analysed. While the third-party privacy seal (lock) and brand do not show effects of someone disclosing their information, the device category shows a highly significant mean difference and therefore accepts the alternate hypothesis that a device category (mobile or desktop) can impact disclosure. The results of this effect are depicted on the graphs below.

Table 11 Device Category; weighted means



A Games Howell post-hoc test was run due the graph bars, in the above graph (table 11, having different widths, which shows that the variances are all different across device categories. The Games Howell past-hoc test takes into account that variances are not the same ensuring they are interpreted in the same way. From the above it is evident, through bars labelled a, b, c, that more data subjects disclosed personal information on the desktop than on a mobile or tablet device. According to the Games Howell bars above, this is show that over 30 people disclosed personal income on their desktop, fewer than ten on their mobile phones and a maximum of two on their laptop.

Table 12 Games Howell post hoc test results

LSD test; variable Lead (Goal 1 Completions) (Spreadshe Probabilities for Post Hbc Tests Error: Between MSE = 31.422, df = 10.000				
Cell No.	Device Category	{1}	{2}	{3}
		32.333	8.8333	1.6667
1	desktop		0.00	0.00
2	mobile	0.00		0.02
3	tablet	0.00	0.02	

All three devices show a significant difference between the leads that came from each of

them. The alternate hypothesis that disclosure of personal information across devices will be different to each other is therefore accepted.

5.2.4 Hypothesis 4

This section examines whether gender differences exist when disclosing personal information within the online context.

First the difference in clicks on the e-mail advertisements between males in Group A (lock) and Group B (no-lock) as well as females in Group A (lock) and Group B (no-lock), is tested and finally the gender differences in clicks is tested through the chi-square two table test.

Males

Table 13 chi-square two-way test and summary table of observed frequencies across male data subjects' responses in Click through rates.

Marked cells have counts > 10. Chi-square (df=1)=160.60, p=0.0000			
Lock/No Lock	Clicked NO	Clicked YES	Row Totals
No Lock	24016	86	24102
Row %	99.64%	0.36%	
Lock	23847	338	24185
Row %	98.60%	1.40%	
Totals	47863	424	48287

Here the null hypothesis, that there is no difference between Group A and Group B for males, is rejected as the P value below 0.05% (0.0000) which shows a significant difference between those that clicked in Group B (no lock) and Group A (lock), with Group

A having the higher click-through rate. This therefore depicts an association between the third-party privacy seal (lock) and the data subjects clicks.

Females

Table 14 chi-square two-way test and summary table of observed frequencies across female data subjects' responses in Click through rates.

Marked cells have counts > 10. Chi-square (df=1)=247.15, p=0.0000			
Lock/No Lock	Clicked NO	Clicked YES	Row Totals
No Lock	41199	165	41364
Row %	99.60%	0.40%	
Lock	40684	579	41263
Row %	98.60%	1.40%	
Totals	81883	744	82627

Here the null hypothesis, that there is no difference between Group A (lock) and Group B (no- lock) for females, is also rejected as the P value below 0.05% (0.0000) which shows a significant difference between those that clicked in Group B (no lock) and Group A (lock), with Group A having the higher click-through rate. This therefore depicts an association between the third-party privacy seals (lock) and consumers' clicks.

Although for both males and females there was a significant difference in the response of both Group A (lock) and Group B (no lock), this is not true for the difference between the genders as shown in chi-square test (table 15) below.

Males vs. Females

Table 15 chi-square two-way test and summary table of observed frequencies across gender data subjects' responses in Click through rates

Marked cells have counts > 10. Chi-square (df=1)=0.17, p=. 67787			
Gender	Clicked NO	Clicked YES	Row Totals
M	47863	424	48287
Row %	99.12%	0.88%	
F	81883	744	82627
Row %	99.10%	0.90%	
Totals	129746	1168	130914

The Null hypothesis, that there will be no difference in clicks between genders in Group A and Group B, is accepted due to there being no significant difference as signified by the P value being greater than 0.05%. (P value is 0.67787).

Secondly the difference in disclosure between males in Group A (lock) and Group B (no-lock) as well as females in Group A (lock) and Group B (no-lock), and then the gender differences in disclosure is tested.

Males Lock/No Lock | Disclose Income

Table 16 chi-square two-way test and summary table of observed frequencies across male data subjects' disclosure related to lock v no lock

Marked cells have counts > 10. Chi-square (df=1)=1.66, p=. 19763			
Lock/No Lock	Disclose Income NO	Disclose Income YES	Row Totals
No Lock	24095	7	24102
Row %	99.97%	0.03%	

Lock	24182	3	24185
Row %	99.99%	0.01%	
Totals	48277	10	48287

The Null hypothesis, that there will be no difference in disclosure between Group A and Group B for males, is accepted due to there being no significant difference as signified by the P value being greater than 0.05%. (P value is 0.19763). This therefore depicts that there is no association between the third-party privacy seals (lock) and consumers disclosure

Females- Lock/No Lock | Disclose Income

Table 17 chi-square two-way test and summary table of observed frequencies across female data subjects' disclosure related to lock v no lock

Lock/No Lock	Marked cells have counts > 10. Chi-square (df=1)=0.00, p=. 99662		
	Disclose Income NO	Disclose Income YES	Row Totals
No Lock	41358	6	41364
Row %	99.99%	0.01%	
Lock	41257	6	41263
Row %	99.99%	0.01%	
Totals	82615	12	82627

While the null hypothesis for females is accepted, the results for females are also insignificant, it seems the lock and no lock had more similar reactions from Group A and Group B than for males (p value is 0.99662)

Males vs. Females – Income disclosure

Table 18 chi-square two-way test and summary table of observed frequencies across gender data subjects' responses in Click through rates

Marked cells have counts > 10. Chi-square (df=1)=0.68, p=. 41091			
Gender	Disclose Income NO	Disclose Income YES	Row Totals
M	48277	10	48287
Row %	99.98%	0.02%	
F	82615	12	82627
Row %	99.99%	0.01%	
Totals	130892	22	130914

The Null hypothesis, that there will be no difference in disclosure between genders is accepted due to there being no significant difference as signified by the P value being greater than 0.05%. (P value is 0.41091).

5.3 Summary of the results

Ultimately the results show that while a third-party privacy seal (lock) may have an impact on consumer behaviour, it is not enough of a high value signal to cause disclosure of personal information. It can be inferred from the results that Privacy concerns on the internet are still rife and even a contextual change such as the device a person is using can spark consumers vulnerability and privacy concerns. The results are discussed in more detail through Chapter 6 below.

CHAPTER 6

6 DISCUSSION OF RESULTS

6.1 Introduction

This chapter provides a discussion and analysis of the results presented in Chapter 5. The sections of the chapter detail different analytical insights relating to key elements of the hypotheses. These are explained through reference to the key elements of hypotheses and their related findings within the context of the applicable literature.

6.2 Summary

An experimental study within the context of using third-party privacy seals (lock) on e-mail advertisements to influence the consumer towards disclosure of private information, was embarked on in light of literature attesting to a positive influence of third-party privacy seals (lock) on consumer privacy concerns and trust regarding the Internet (Mothersbaugh et al., 2012; Özpölat & Jank, 2015).

The experiment sought, *inter alia*, to test the hypotheses of using third-party privacy seals (lock) within e-mail advertisements to positively influence disclosure by consumers of their private information. This study analysed several findings from the academic literature in the context of signalling theory and online advertising that third-party privacy seals (lock) would positively influence the trust concerns as well as the privacy concerns of consumers, which would ultimately result in consumers being more likely to disclose their private information (Kim & Kim, 2011; Mavlanova et al., 2012; Özpölat & Jank, 2015).

As seen in Chapter 5 results of the study concurred with previous literature that while a third-party privacy seal (lock) may have an impact on consumer behaviour, it is not enough of a high value signal to cause disclosure of personal information and future research as well as companies within the internet space will need to experiment with how to enable consumers to feel their information is being correctly managed and less

vulnerable on the internet.

It can be inferred from the results that privacy concerns on the Internet are still rife and even a contextual change, such as the device a person is using or the brand that is speaking to them, can set off consumer's vulnerability and privacy concerns. The results are discussed below for each hypothesis and then summarised at the end of the chapter leading into the conclusions.

6.3 Hypothesis 1: A third-party privacy seal (lock) is a high value signal, and will result in consumer disclosure.

The study's first objective sought to show that the high-value of a third-party privacy seal (lock) would positively influence the disclosure behaviour of consumers (Mavlanova et al., 2012). The results, however, showed that there was no significant association between the lock on the e-mail and the disclosure of personal information. From the findings, it is noted that while the hypothesis does not hold true that a lock is a high-value signal in influencing consumer disclosure.

Possibly we see no difference in Group A and Group B because people, in South Africa, do not trust that the third-party privacy seal (lock) protects them from online fraud and security that is so common in our daily media and financial institutions. ACSSE is an initiative undertaken by the University of Johannesburg and the Academy of Computer Science and Software Engineering, to study online crime on the African continent with specific reference to South Africa (Fichardt, C, 2015). This study investigated phishing scams in particular. The research found that South African citizens have been affected mostly by banking related fraud including as phishing scams the most common. A phishing scam was defined by Acquisti et al. (2011, p.867) as e-mail that attempts "to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity".

There was a difference in the number (although slight) of consumers that disclosed their income across the bases, which showed a slight a negative influence when there is a lock on an e-mail advertisement, and the advertisement is not in a relevant context. A third-party privacy seal (lock) may therefore act as a low-value signal, which can cause privacy

concerns and hinder consumer disclosure. While there was no statistical significance in the difference between Group A and Group B, the % per base was different based on the affinity of the base.

This finding is similar to academia relating the influence of personalisation of advertising and privacy concerns (Bleier & Eisenbeiss, 2015; Tucker, 2014; van Doorn & Hoekstra, 2013; Xu et al., 2011). Van Doorn and Hoekstra (2013, p.339) specifically found that personalisation on advertisements was a “double-edged sword” as it needed to be relevant to the consumer to positively impact their purchase intention. Understood in this light, the study can be looked at in the context of the consumers:

- *Base J* is a database for a service that provides marketing around entertainment and third parties use this as a way to market to advertisers and had below a 0.01% disclosure rate.
- *Base H* and *Base Y* are financial service affinity bases and both had between a 0.06% and 0.10% disclosure rate.

The e-mail advertisement that was used, advertised financial services products, and therefore *Base H* and *Base Y* affinity. It can be inferred that due to the fact that they had used the company’s services for financial services previously, they were more likely to disclose their information.

Base J, although it has an affinity to the company, may never have been exposed to the financial services products of the company previously.

Aguirre et al. (2014) explained that when consumers disclose their private information, they are acting as “rational economic agents” engaging in a cognitive cost-benefit analysis (Aguirre et al., 2014 p.37). This also speaks to the privacy-paradox that exists for consumers on the Internet (Pavlou, 2011; Tucker, 2012; Xu et.al, 2011). Tucker (2012) stated that the privacy-paradox reveals the consumer contemplating the benefit associated with their risk, in disclosure of their information being worth what they will get in return. *Base J* may have valued the risk differently or viewed the benefit as being too small compared to the significantly sensitive information they would need to disclose.

In the study by Xu et al. (2012, p.17) on privacy assurances, perceived control and privacy concerns, it was suggested that individuals may not regard industry self-regulators as “powerful others that can exercise proxy control for them”. Consumers may perceive little benefit in seeking recourse from these third party bodies should their information be misused.

This is especially plausible in light of the South African context where the Government legislation protecting consumers and their privacy concerns (via the Consumer Protection Act and Protection of Personal Information Act) have been timeous in their implementation as well as industry governance, with industry bodies so far having done little to help hasten the implementation. A recent example of this was the Wireless Application Service Providers (WASPs) in South Africa unlawfully billing consumers to “opt out” marketing. Neither the law enforcement officials, nor the industry body (WASPs) have responded to the consumer concerns and complaints surrounding the issue (mybroadband.co.za, 2015 September). Price Waterhouse Coopers Global Economic Crime Survey, 2014, found that South African companies experience more fraud and bribery than anywhere else in the world. Much of this fraud is linked to crime within the internet environment (BEETAR. M, 2014) This survey found that globally over 600,000,000.00 customer information records have been fraudulently accessed. This links with the findings of the first hypothesis, as it appears that online users are circumspect when committing personal information online.

Another possible explanation could lie in the interpersonal interaction element of MDT. By introducing the “existence” of another through a third-party privacy seal (lock), consumers may be alerted to the privacy concerns and control around how another is managing their personal information (Hong, 2013, pg.277). While the MDT theory proposed that the third-party certification signals to consumers that a website’s information practices are in line with industry privacy standards and therefore their products are of a certain quality or standard. On the flip side, this signal may identify the need for the existence of another party to watch over the actions of a company, which alerts the consumers’ to their lack of control over their private information further (Lwin and Williams, 2003, p.267).

Signalling theory’s underlying principle has been described as the use of a costly signal (i.e., must have a cost to the signaller) sent for the signaller’s benefit (of anticipated revenue from the receiver), while the receiver uses the signal as a true reflection of the

claims made by the retailer, otherwise the cost of the signal is not strategic (Connelly et al., 2011; Mavlanova et al., 2012). While Liberali et al. (2013, p.103) identified that through signalling, consumers' feelings of risk linked with information asymmetry on the Internet could be minimised as they identified a third-party privacy seal as a 'high-quality, the actual cost of the signal on the signaller needs to be considered. The cost of the third-party privacy seal (lock) may not be viewed by the online consumer as a high enough burden on the company to balance the disclosure of private information and, therefore, may not be viewed as a high-value signal by consumers.

In disclosing private information online, literature had noted that it is important for the company to create an environment where the consumer can easily and readily identify how their information is controlled, managed and what may put a consumer at risk (John et al., 2011; Pavlou, 2011). Another plausible explanation of why the third-party privacy seal (lock) may have had no influence at all, as seen in *Base H*, may be that the consumer does not know what the third-party privacy seal (lock) denotes. This would mean that further information relating to the privacy policy of the advertiser needs to be published on the e-mail advertisement at the same time as the third-party privacy seal (lock).

6.4 Hypothesis 2: A third-party privacy seal (lock) will result in a higher click-through rate on an e-mail advertisement

E-mail advertisements have been found to be mistrusted and linked to eliciting consumer privacy risks due to their common association with "spam" advertising (Kim & Kim, 2011). While The second hypothesis showed a significant difference between clicks in group A and Group B, in that more people who were sent the e-mail advertisement containing the third-party privacy seal (lock) (Group A) clicked on the e-mail than those who received the e-mail advertisement without the third-party privacy seal (lock) (Group B). This therefore proved the second alternative hypothesis, which stated that, Group A will have a higher click-through rate (i.e., more consumers will click on the e-mail links). This hypothesis therefore concurs with the Mothersbaugh et al. (2012) that e-mail is linked to consumer privacy concerns (Kim & Kim, 2011).

However, it is important to note the difference between the Bases responses within these

results. Our results show opposing views with regards to Kim & Kim's 2011 study (p.154) which tested and found that that third-party privacy seal (lock) were operative in transferring trust for consumers when used on an advertisement (as opposed to a website). *Base H* did not have any association between the third-party privacy seal (lock) (lock) and click-through rate, as opposed to both *Base Y* and *Base J* which both depicted a significant association between the click-through on Group A (with the lock) and Group B. While both *Base H* and *Base J* showed an association, these associations had different results in that:

- For *Base Y*, (a financial services base) there were more clicks in Group B (which did not contain the third-party privacy seal (lock)) than in Group A, while *Base J* (an entertainment base) had more clicks in Group A than In group B (with the lock).

This implies that the lock (third-party privacy seal) can have a positive or a negative connotation with privacy concerns based on the context of the advertisement. . This may speak to the facts that while more consumers are choosing to share their personal information online it is not without concern (Spiekerman et al., 2015). Aguirre et al. (2015) alluded to the association of consumers' assumption that they could trust the source of the personalised advertisement more when the advertisement appeared within credible contexts or incorporated information icons that signalled trustworthiness. This may suggest that the third-party privacy seal (lock) not being enough of a signal on its own. The context of the advertisement being an e-mail advertisement identified by consumers as signalling spam (Kim & Kim, 2011), along with the brand advertiser (Brand Y) belonging to the financial services industry, an industry known to have high obtrusive rates regarding advertisements, may be the result of a context that is not viewed as credible.

As discussed above within the South African context both ACCSSE research (Fichardt, C, 2015), and Price Waterhouse Coopers Global Economic Crime Survey (BEETAR. M, 2014) eluded to the concerns South Africans have surrounding their personal information specifically within the realms of e-mail marketing (phishing scams) and financial services fraud. Acquisti et al. (2011, p.867) studied phishing scams within their research and alluded to individuals being more likely to disclose their personal information in contexts

that downplay privacy concern even if the context is objectively higher in perceived disclosure risk.

Spiekerman et al. (2015) identified the need for companies to ensure that they create more trustworthy relationships with their consumers, in order to counter-effect consumers feelings of vulnerability and privacy concerns and the use of a third-party privacy seal (lock) may not be sufficient to achieve this. As stated previously, additional information may need to be published together with the seal, which informs the consumer that the seal means their information is stored and managed according to a high standard, ensuring that control exists.

The mediating effect of trust impacting consumer disclosure of private information in the context of online privacy concerns could not be established through this study. While third-party privacy seal (lock) are identified in the electronic commerce literature as strategic and effective tools in enhancing consumer trust towards a brand, as well as a tool in managing consumers' privacy concerns (Özpolat & Jank, 2015), our research did not prove the association across all brands..

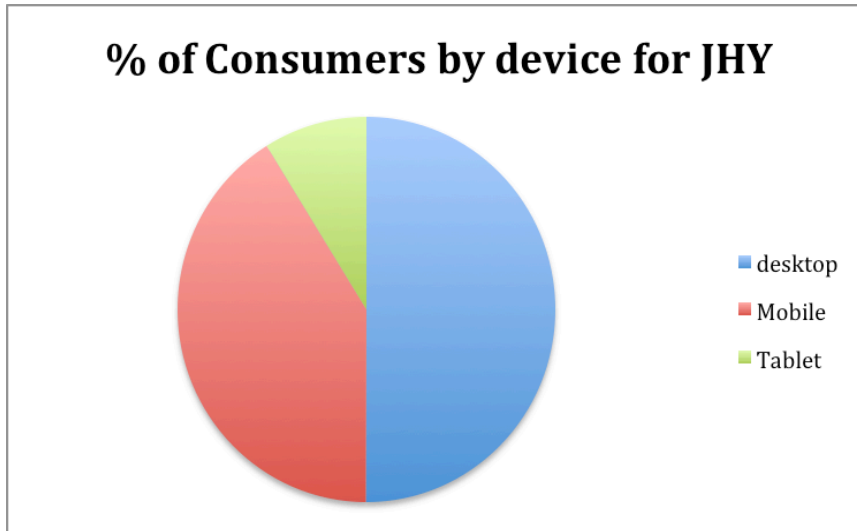
6.5 Hypothesis 3: Desktop, Mobile and Tablet

The third hypothesis examines whether different settings activate privacy concerns differently and will lead to different levels of disclosure. It looked at discovering more insight into the previous literature suggesting this be studies, all else being the same with respect to the objective costs and benefits of disclosure (John et al., 2011). It, was therefore, hypothesised that consumers disclosure was linked to the device they were using to access the website. Due to Özpolat and Jank (2015, p.55) call for more data, data to discuss findings around devices was analysed in order to add to the growing body literature. This is by no means conclusive and it is suggested that future research study this in more detail and with more focus on this topic as their main hypothesis.

It is useful to understand the company's data surrounding device usage across JHY brands, before discussing the results of hypothesis 3. This data was pulled through Google Analytics (GA) and summarized below. Company JHY's, Google analytics (GA) data for period of the test, (1 August-1 October 2015), show in figure 7 below that that

their consumer online spilt (for Base H, J and Y) is 50% desktop, 41% mobile and 9% tablet.

Figure 7 Google Analytics stats of JHY device categories for user session, dated 1/08/15-1/10/15



Each base is than further split up as follows:

- Base H – Mobile 48%, Desktop 46%, Tablet 6%
- Base Y - Desktop 61%, Mobile 25%, Tablet 13%
- Base J – Desktop 50%, Mobile 42%, Tablet 9%

Here the alternate hypothesis that disclosure of personal information across devices will be different to each other was accepted. The Games Howell past-hoc test showed that over 30 people disclosed personal income on their desktop, fewer than ten on their mobile phones and a maximum of two on their laptop.

The means between the devices was shown to have significant disclosure based on the device used, and these differences were significant across all three devices. From figure 7, it is evident that per device:

- Desktop had the most significant lead volume with mobile having significantly less and the tablet having the lowest volume.
- The tablet makes most sense, as it is the least used device across the brands, as shown in the Google Analytics (GA) stats. The mobile and desktop lead volumes however are not consistent with company statistics discussed above.

From this it can be assumed that the device impacted the decision of the consumer to disclose their information. Again the third-party privacy seal (lock) had no effect on the consumers disclosure, as was evident from the interaction effect between devices which tested if Group A or Group B had differing data, and found that the data was the same across both e-mail advertisement groups.

Ström et al., (2014, p.1007) stated that the size of the screen plays a role in usage across desktop and mobile. The website was responsive (fits to the screen size you are viewing the website on, through a computer code added to the website source code) and therefore the screen was visible on all devices, however this was not tested and is therefore a limitation to this study. However the Google Analytics (GA) pulled above show that generally there are more mobile users on the website than what the lead volume would suggest. It can be assumed that although screen size may have been one of the reasons that lead volumes were lower, it is not the only reason.

In relation to the South African context, the findings within this research, of the data subjects apprehension in giving information on a mobile device being more prominent than their apprehension on a website, aligns with the study previously quoted via the Price Water House Coppers Global Economic Crime Survey 2014 (BEETAR. M, 2014). The Price Water House Coopers study, spoke to the demand for hand-held devices to contain sophisticated anti-fraud technology, due to the common mistrust and concern surrounding access and misuse of personal information on these devices. The scope of this research concurred with this study in that the data showed, that more of the data subjects disclosed their personal information on a desktop than did on a mobile phone or tablet (both of which are hand-held) devices.

The results seem to concur with Keith, et al. (2013, p.1172) study which found that perceived privacy risks played a larger role than perceived benefits in determining

disclosure intentions on mobile than on a desktop. The privacy-paradox is suggested as a reason for this as the risk to data being taken may not be worth the benefit for a consumer receiving a service. The risk may be perceived as higher when accessing through a desktop and the suggestion that Dienlin & Trepte, (2015) had that the privacy-paradox is a relic of the past may just be context based and not holistically tested.

6.6 Hypothesis 4: Gender differences

This hypothesis examined whether gender differences exist when disclosing personal information within the online context. We discuss this in relation to two sub hypotheses being information disclosure and clicks on the e-mail advertisement.

Jansen et al. (2013) identified that while traditionally responses between genders were significantly different within the advertising context, for example that men and women reacted and responded to personal questions as well as stimuli such as schema and images versus text Acquisti et al. (2012). This significant difference is not so evident within the online context. Our results corroborated with Jansen et al. (2013), as we found no significant difference in clicks and disclosure of information between the genders.

The only slight difference we found, that is worth noting was in the number of females that disclosed personal information compared with number of males, in that 0.03% of males disclosed their personal information while 0.01% of females disclosed their personal information, which could speak to the findings in Acquisti et al. (2012) that males and females respond different to disclosing their personal information in that men are less concerned of the risk. Unfortunately this study was limited as we could only use Base J for the analysis due to the fact that Base H and Base Y did not have this data prepopulated. We were able to look at the Google analytics (GA) data that JHY used for their own records in analysing the campaign.

Google Analytics (GA) , though an external tracking tool, uses the nominal data to help companies measure their campaigns and allows selection of any subset of data (Manovich, 2011) . We pulled the data surrounding gender behaviour that was relevant to the campaigns. As detailed in chapter 4, The Google Analytics (GA) measurement tag was placed on the relevant pages on the website to track the e-mail advertisements. We

used this data in the below discussion, The period over which the e-mail was sent across all three sends was selected, 1 August 2015 to 1 October 2015, for analyses (Pakkala, Presser, & Christensen, 2012).

Table 19 and table 20 below are the Google Analytics (GA) results for the campaigns across both bases. It shows the Brands per Group and how the females and males responded. Google defines a session as “ a group of interactions that take place on your website within a given time frame” refers to the number of data subjects that interacted with the website arriving directly from clicking on the e-mail advertisement. Google defines Goals measured (i.e. leads) as “how well your site or fulfils your target objectives and represents a completed activity, called a conversion, that contributes to the success of your business”. For the campaign JHY had defined a goal as a lead, which referred to the action of disclosing income.

The data is limited to fewer results (i.e. number of reported session sand leads) due to GA’s protection of personal information policies. These policies ensure that Google keep results as general (broad) as possible so companies cannot trace back individual information of a specific consumer.

Table 19 Base Y Gender Google Analytics results for Group A and Group B

Brand	Campaign	Gender	Sessions	Lead
Base Y	Group A	female	28	9
Base Y	Group A	male	19	11
Base Y	Group B	female	39	9
Base Y	Group B	male	27	5
			113	34

Table 20 Base Y Gender Google Analytics results for Group A and Group

Brand	Campaign	Gender	Sessions	Lead	(Goal	1
-------	----------	--------	----------	------	-------	---

				Completions)
Base H	Group A	female	45	16
Base H	Group A	male	25	10
Base H	Group B	female	65	13
Base H	Group B	male	29	9
			164	48

Table 21 and 22 were used in order to create the bar chart below of % of gender per lead and sessions across both base sends.

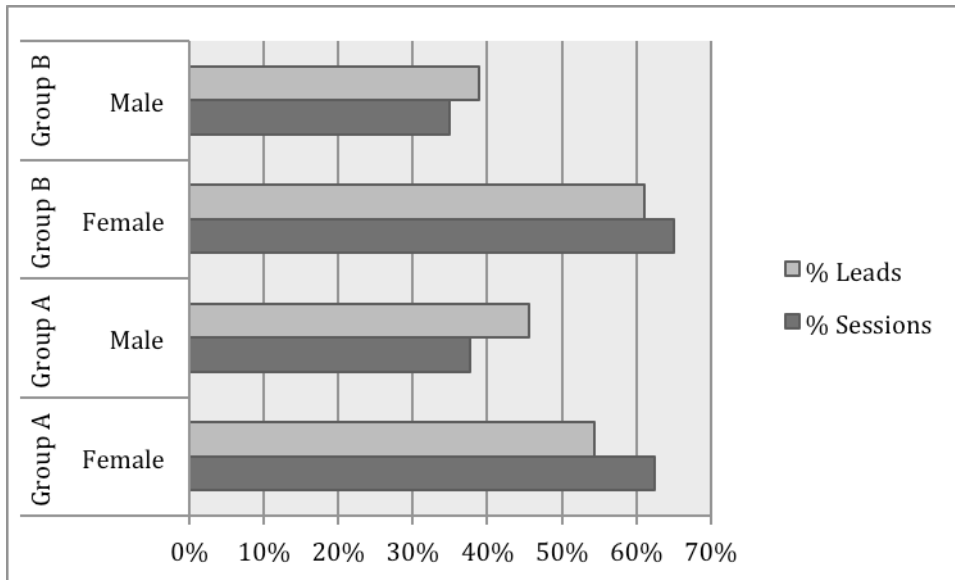
Table 21 Base Y Gender % per Group

Campaign	Gender	Sessions	Insurance Lead (Goal 1 Completions)	% OF TOTAL LEADS	% OF TOTAL SESSIONS
GROUP B	female	39	9	64%	59%
GROUP B	male	27	5	36%	41%
GROUP B	TOTAL	66	14		
GROUP A	female	28	9	45%	60%
GROUP A	male	19	11	55%	40%
GROUP A	TOTAL	47	20		

Table 22 Base H Gender % per Group

Campaign	Gender	Sessions	Lead (Goal 1 Completions)	% OF TOTAL LEADS	% OF TOTAL SESSIONS
GROUP A	female	45	16	62%	64%
GROUP A	male	25	10	38%	36%
GROUP A	TOTAL	70	26		
GROUP B	female	65	13	59%	69%
GROUP B	male	29	9	41%	31%
GROUP B	TOTAL	94	22		

Figure 8 % Gender leads and sessions splits for both Base Y and Base H, Group A and Group B



The Google analytics results (figure 8) show a difference between session to lead ratio between males and females. This is depicted in that more males seem to disclose their information than females do when looking at lead% compared to session % i.e. the lead % is always higher in males than it is in females when looking at it in comparison to session% (the light grey graph for males is always a higher % than the dark grey Bar for sessions for males). Though not conclusive by any means, it would seem that men are more inclined to disclose personal details than woman. This may speak to Acquisti et al. (2012, p.35) findings that gender differences exist between genders response to personal questions. While Acquisti et al. (2012) findings were highly significant we do believe there is some truth to it in the above data.

Acquisti et al. (2012, p.35) also concluded that men were much more consistent among themselves in their general response, but women differed quite substantially between them in their responses. This was not evident in either sets of our results and seems to corroborate with Jansen et al. (2013) view that online advertising may not have the gender response difference that we are used to from traditional advertising.

6.7 Conclusion

The objective of the study aimed to answer is whether a third party seal, when used, as a signal in an e-mail advertisement, will influence consumers' behaviour, specifically in relation to disclosure of private information. While the results did not find that a third-party privacy seal (lock) in an e-mail advertisement impacts consumer's disclosure of their private information, several findings did show impacts of third-party privacy seal (lock) and consumer behaviour indicating that privacy concerns are still very relevant to the context of the internet and need to be explored further by the research and companies to find ways to mitigate the impact. This is discussed further in the concluding chapter of the research.

CHAPTER 7

7 CONCLUSION

7.1 Introduction

This chapter highlights the main findings of the research, which set out to empirically test the impact of a third-party privacy seal on an e-mail advertisement, in an effort to understand its impact on consumer disclosure of private information. It also includes recommendations based directly on these findings for both companies and marketers. Recommendations for future research and limitations of the research will also be discussed.

7.2 Findings

The research aimed to empirically experiment with the concepts of firstly, a third-party privacy seal being effective for companies to use in their advertising, in generating consumer's disclosure of personal information and secondly privacy concerns and consumer mistrust surrounding personal information on the internet, in order to further explore and understand the live landscape of the internet. Finally, the research added scope and robustness through a live experiment within the environment by providing research relating to device implications for users as well as gender differences in response to advertising and disclosure of information online.

The research contributed to the growing body of research of third-party privacy seal (lock) While a third party seal has enough value to generate consumer trust and cause consumers to click on an advertisement, it does not have the same high-value for consumers in generating disclosure of personal information.

The research further added to the body of knowledge surrounding mistrust of third-party privacy seal (lock) within advertisements. While for certain brands the research found experimental evidence for that there is truth in the value of third-party privacy seal (lock) generating trust and clicks on advertisement, as per the literature prior, the third party seal

(lock) when used as a signal can also have a negative impact if used by a brand that is not trusted or known by the consumer to be a trusted brand as alluded to by Aguirre et al. (2015) research. This was clear in the difference between Brand Y and Brand J, which both showed that there was a significant difference in clicks on the e-mail advertisements however for Brand Y the consumers were less inclined to click on the advertisements if it contained a lock while on Brand J they were more inclined to click on the advertisements that contained a lock.

There was a difference in disclosure based on the device a consumer was using with more consumers disclosing information via desktop than via a mobile confirming and adding to the recent body of knowledge on hand-held devices and privacy concerns.. This result showed that majority of the disclosure came from desktops devices as opposed to mobile devices, and very few from tablet devices. The results, over this period, showed 50% desktop device, 41% mobile device, and 9% from a tablet device. This research therefore gives empirical evidence that desktop users are more likely to disclose their personal income than mobile users and gives significant insight as well as avenues for future research.

Gender differences are not as evident in the online context as they are offline as per hypothesis 4 of this research; there was no difference between disclosure of information by males and females. This adds to new findings that explore the difference between the gender reactions to traditional advertising and Internet advertising.

7.3 Recommendations

Recommendations for marketing practitioners and companies are listed below in light of the findings.

Spiekermann et al., (2015) highlighted the power that companies have in helping to create a safe environment for consumers, where consumers feel less vulnerable around their privacy concerns. Research has recommended companies use high-value signals such as third-party privacy seal (lock) to facilitate this management (Mavlanova et al., 2012; Wells et al., 2011, Kim & Kim, 2011). The results were that a third-party privacy seal would not create enough of a signal for consumers to disclose their information, whether this is for a

benefit or not, highlighting the need for companies to manage privacy concerns much more strategically.

What this means for marketing practitioners, is that while more consumers are choosing to share their personal information online consumer mistrust and concerns surrounding their personal information are still very much a reality and will have to be considered very seriously for companies to ensure they get a return on marketing investments (Tucker, 2012; Roeber et al, 2015; Spiekerman et al, 2015). The sensitivity of information being requested needs to be identified by companies, as highly sensitive information (such as income) leads to increased consumer privacy concern. It is recommended that marketing practitioners first identify what personal information is essential for a campaign and only request highly sensitive information if it is vital.

The research did show that while a third-party privacy seal (lock) may not be enough of a signal for consumer disclosure it is a high-value signal for consumers to take an action (such as clicking) on an advertisement. It is therefore recommended that marketer use third-party privacy seal (lock) within their marketing plan in order to grow brand affinity and consumer trust and to get an action on an advertisement. Once a consumer takes action on an advertisement, it is recommended that marketing practitioners ensure this environment is continued and they consider additional trust and privacy signals. For example, Xu et al. (2012, p.17) found that consumers do not trust third-party bodies to protect them and inferred that consumers may perceive little benefit in seeking recourse from these third-party bodies should their information be misused. It is therefore recommended that companies use several trust symbols to signal to consumers that their privacy is protected but at the same time attempt to downplay the concerns of the individual surrounding their privacy (Aguirre et al., 2015). They can potentially do this by focusing on more positive aspects such as showing how many people have used and trusted their website, as opposed to focusing on negative aspects such as showing a user that they use precaution preventing fraudulent activity which may put their private information at risk.

It is recommended that marketing practitioners manage and understand the devices their consumers are using to access their advertisements and websites, as the study's findings understood that perceived privacy risks played a larger role on a mobile than on a

desktop.

Jansen et al. (2013) identified that while traditionally responses between genders were significantly different within the advertising context, this significant difference is not so evident within the online context and our results identified with this research. While our study and this topic has been detailed in limitations and recommendations for future research, it is recommended that marketing practitioners experiment with this within their marketing initiatives, specifically if they are targeting only one of the genders. This is due to. Acquisti et al. (2012) study which found that that males and females respond different to disclosing their personal information, in that men are less concerned of the risk and our research insinuated that is my be valid.

7.4 Managerial Implications

Access and collection of consumers' private information is essential for companies trading on the internet, as well as companies competing within the global landscape, to remain competitive. With personal information being a commoditized asset, the effective management of the data (private information) is therefore of paramount importance, not only to compete but also to gain a competitive advantage. Management needs to efficiently identify, administer and track private information required by the company, including the methods of efficiently accessing and managing personal data in a way that does not compromise the brand and consumers perception of the company.

7.5 Limitations of the research and suggestions for future research

This section discusses several limitations of the research, as well as suggestions for future research.

The study only considered a single South African company within the financial services sector, and other industries as well as diverse databases could be used to gain further insights and refinement to the results. A further limitation to the study was that JHY stored its brand databases separately and each brand collected different types of information from its consumers and so one could not test further demographic responses. A qualitative angle to the study would have added further consumer insight into the actions

taken by consumers within the live experiment, as only quantitative data was used in the test, which limited the insights of the research. Although testing a specific type of marketing (an email advertisement for this study) the research added a more refined and concise study and set of results, a less specific study which looked at the entire consumer journey (that is - from advert to website to thank you page to contact of the consumer) of the advertisement may give further insight into ways of positively impacting consumer disclosure of their personal information.

Below are several suggestions for future research:

- Firstly, to track the entire consumer journey by adding additional information (such as privacy policy or positive trust assurance such as other people using the services) and signals information and assessing their impact on the consumer disclosure.
- Secondly, to use several database affinities and advertisements in assessing the impact of consumer disclosure across a variety of consumers
- Thirdly, to further the Acquisti et al. (2012) study alluding to the finding that males and females respond different to disclosing their personal information in that men are less concerned of the risk.
- Fourthly, to use post-test or pre-test qualitative survey identifying the view of third-party privacy seal (lock) and then the link (if any) between third-party privacy seal (lock) and the consumers' choice to disclose their personal information.
- Finally, to implement and track consumer disclosure across devices (mobile, tablet and desktop).

7.6 Conclusion

The free-flow of information created by the Internet has rapidly expanded a company's ability to access consumers' and individuals' personal information increasing the need for companies to gain access to such information in order to remain competitive. Companies signal that they manage consumer's personal information, according to the required standards of the industry by using third-party privacy seals. Although this signal has been found to be effective in impacting consumer behaviours, this study did not find that they are of a high enough value to impact consumer disclosure when used in an e-mail

advertisement.

REFERENCE LIST

- Acquisti, A., John, L. K. & Loewenstein, G. (2012). The Impact of Relative Standards on the Propensity to Disclose. *Journal of Marketing Research*, 49(2), 160–174. <http://doi.org/10.1509/jmr.09.0215>
- Aguirre, E., Mahr, D., Grewal, D., Ruyter, K. De & Wetzels, M. (2015). Unravelling the Personalization Paradox : the Effect of Information Collection and Trust-Building Strategies on Online Advertisement Effectiveness. *Journal of Retailing*, 91, 34–49.
- Atkinson, L. & Rosenthal, S. (2014). Signalling the Green Sell: the Influence of Eco-Label Source, Argument Specificity, and Product Involvement on Consumer Trust. *Journal of Advertising*, 43(1), 33–45. <http://doi.org/10.1080/00913367.2013.834803>
- Babin, B. J. & Babin, L. (2001). Seeking Something Different? A Model of Schema Typicality, Consumer Effect, Purchase Intentions and Perceived Shopping Value. *Journal of Business Research*, 54(2), 89–96. [http://doi.org/10.1016/S0148-2963\(99\)00095-8](http://doi.org/10.1016/S0148-2963(99)00095-8)
- Baek, T. H. & Morimoto, M. (2012) Stay Away From Me, *Journal of Advertising*, 41(1), 59-76, DOI: 10.2753/JOA0091-3367410105.
- Bandyopadhyay, S. (2009). Antecedents and Consequences of Consumers' Online Privacy Concerns. *Journal of Business and Economics Research*, 7(3), 41–48.
- BEETAR, M (2014). Sa companies' fraud stats lead the world. <http://www.bdlive.co.za/business/2014/12/10/sa-companies-fraud-stats-lead-the-world>
- Bleier, A. & Eisenbeiss, M. (2015). The Importance of Trust for Personalized Online Advertising. *Journal of Retailing*, 1–20. <http://doi.org/10.1016/j.jretai.2015.04.001>
- Boulding, W. & Kirmani, A. (1993). A Consumer-Side Experimental Examination of Signalling Theory: Do Consumers Perceive Warranties as Signals of Quality? *Journal of Consumer Research*, 20(1), 111. <http://doi.org/10.1086/209337>
- Connelly, B. L., Certo, S. T., Ireland, R. D. & Reutzel, C. R. (2011). Signalling Theory: A

- Review and Assessment. *Journal of Management*, 37(1), 39–67.
<http://doi.org/10.1177/0149206310388419>
- Dienlin, T. & Trepte, S. (2015). Special section article : Putting the Social (Psychology) into Social Media: is the Privacy Paradox a Relic of the Past ? An in-depth Analysis of Privacy Attitudes and Privacy Behaviors, 297 (November 2013), 285–297.
- Fichardt, C. (2015) Just how big a threat is cybercrime to SA.
<http://www.bdlive.co.za/business/technology/2015/06/08/just-how-big-a-threat-is-cybercrime-to-sa>. Doi: <http://adam.uj.ac.za/csi/ - /20152/11/>
- Goldfarb, A. & Tucker, C. (2011). Rejoinder-Implications of “Online Display Advertising: Targeting and Obtrusiveness.” *Marketing Science*, 30(3), 413–415.
<http://doi.org/10.1287/mksc.1100.0634>
- Goldfarb, A. & Tucker, C. (2012). Shifts in Privacy Concerns. *American Economic Review*, 102(3), 349–353. <http://doi.org/10.1257/aer.102.3.349>
- Goodrich, K. (2014). The Gender Gap: Brain-processing Differences Between the Sexes Shape Attitudes About Online Advertising. *Journal of Advertising Research*, 54(1), 32–43. <http://doi.org/10.2501/JAR-54-1-032-043>
- Hann, I., Hui, K., Lee, S.-Y. & Png, I. (2007). Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach. *Journal of Management Information Systems*. <http://doi.org/10.2753/MIS0742-1222240202>
- Hong, W. (2013). Research Note: Internet Privacy Concerns : An Integrated Conceptualization And Four Empirical Studies 1. *MIS Quarterly*, 37(1), 275–298.
- Hu, X., Wu, G., Wu, Y. & Zhang, H. (2010). The Effects of Web Assurance Seals on Consumers' Initial Trust in an Online Vendor: a Functional Perspective. *Decision Support Systems*, 48(2), 407–418. <http://doi.org/10.1016/j.dss.2009.10.004>
- Jansen, B. J., Moore, K. & Carman, S. (2013). Evaluating the Performance of Demographic Targeting Using Gender in Sponsored Search. *Information Processing and Management*, 49(1), 286–302. <http://doi.org/10.1016/j.ipm.2012.06.001>
- Jocz, K.E. & Quelch J.A (2008) An Exploration of Marketing's Impacts on Society: A Perspective Linked to Democracy. *Journal of Public Policy & Marketing*, 27(2), 202-206. <http://dx.doi.org/10.1509/jppm.27.2.202>

- John, L. K., Acquisti, A. & Loewenstein, G. (2011). Strangers on a Plane: Context-dependent Willingness to Divulge Sensitive Information. *Journal of Consumer Research*, 37(5), 858–873. <http://doi.org/10.1086/656423>
- 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. <http://doi.org/10.1016/j.ijhcs.2013.08.016>
- Kim, K. & Kim, J. (2011). Third-party Privacy Certification as an Online Advertising Strategy: An Investigation of the Factors Affecting the Relationship between Third-party Certification and Initial Trust. *Journal of Interactive Marketing*, 25(3), 145–158. <http://doi.org/10.1016/j.intmar.2010.09.003>
- Lavrakas, P. J. (2008). *Encyclopaedia of Survey Research Methods*. A-M, 725–732.
- Leon, P. G., Rao, A., Schaub, F., Marsh, A., Cranor, L. F. & Sadeh, N. (2015). *Privacy and Behavioral Advertising : Towards Meeting Users' Preferences. Symposium on Usable Privacy and Security (SOUPS)*.
- Leon, P. G., Ur, B., Wang, Y., Sleeper, M., Balebako, R., Shay, R. Bauer, L., Christodorescu, M., Cranor, L. F. (2013). *What Matters To Users? Factors That Affect Users' Willingness to Share Information with Online Advertisers. Proceedings of the Ninth Symposium on Usable Privacy and Security - SOUPS '13*, 1. <http://doi.org/10.1145/2501604.2501611>
- Lewis, M., Whittler, K. A. & Hoegg, J. (2013). Customer Relationship Stage and the Use of Picture-dominant Versus Text-dominant Advertising: a Field Study. *Journal of Retailing*, 89(3), 263–280. <http://doi.org/10.1016/j.jretai.2013.01.003>
- Liberali, G., Urban, G. L. & Hauser, J. R. (2013). Competitive Information, Trust, Brand Consideration and Sales: Two Field Experiments. *International Journal of Research in Marketing*, 30(2), 101–113. <http://doi.org/10.1016/j.ijresmar.2012.07.002>
- Lwin, M. O. & Williams, J. D. (2003). *A Model Integrating the Multidimensional Developmental Theory of Privacy and Theory of Planned Behavior to Examine Fabrication of Information Online*. 2, 257–273. <http://doi.org/10.1023/B:MARK.0000012471.31858.e5>
- Mavlanova, T., Benbunan-Fich, R. & Koufaris, M. (2012). Signalling Theory and

- Information Asymmetry in Online Commerce. *Information and Management*, 49(5), 240–247. <http://doi.org/10.1016/j.im.2012.05.004>
- Manovich, L. (2011). Trending: the promises and the challenges of big social data. *Debates in the digital humanities*, 460–475. http://www.manovich.net/DOCS/Manovich_trending_paper.pdf
- Miyazaki, A. D. & Krishnamurthy, S. (2002). Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions. *Journal of Consumer Affairs*, 36(1), 28–49. <http://doi.org/10.1111/j.1745-6606.2002.tb00419.x>
- Mothersbaugh, D. L., Foxx, W. K., Beatty, S. E. & Wang, S. (2012). Disclosure Antecedents in an Online Service Context: The Role of Sensitivity of Information. *Journal of Service Research*, 15(1), 76–98. <http://doi.org/10.1177/1094670511424924>
- Özpolat, K. & Jank, W. (2015). Getting the Most Out of Third Party Trust Seals : an Empirical Analysis. *Decision Support Systems*, 73, 47–56. <http://doi.org/10.1016/j.dss.2015.02.016>
- Pavlou, P. A. (2011). State of the Information Privacy Literature: Where Are We Now and Where Should We Go? *MIS Quarterly*, 35(4), 977–988. <http://doi.org/10.1126/science.1103618>
- Roeber, B., Rehse, O., Knorrek, R. & Thomsen, B. (2015). Personal Data: How Context Shapes Consumers' Data Sharing with Organizations from Various Sectors. *Electronic Markets*, 95–108. <http://doi.org/10.1007/s12525-015-0183-0>
- Saunders, M & Lewis, P (2012). *Doing Research in Business and Management*. Pearson: Edinburgh Gate
- Smith, H. J., Dinev, T. & Xu, H. (2011). Information Privacy Research: an Interdisciplinary Review. *MIS Quarterly*, 35(4), 989–1015. <http://doi.org/10.1126/science.1103618>
- Spiekermann, S., Acquisti, A., Böhme, R. & Hui, K.-L. (2015). The Challenges of Personal Data Markets and Privacy. *Electronic Markets*, 25(2), 161–167. <http://doi.org/10.1007/s12525-015-0191-0>
- Ström, R., Vendel, M. & Bredican, J. (2014). Mobile Marketing: a Literature Review on its Value for Consumers and Retailers. *Journal of Retailing and Consumer Services*, 21(6), 1001–1012. <http://doi.org/10.1016/j.jretconser.2013.12.003>

- Tsai, J. Y., Egelman, S., Cranor, L. & Acquisti, A. (2011). The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. *Information Systems Research*, 22(2)(January 2014), 254–268. <http://doi.org/10.1287/isre.1090.0260>
- Tucker, C. E. (2012). The economics of advertising and privacy. *International journal of Industrial organization*, 30(3), 326-329.
- Tucker, C. E. (2014). Social Networks, Personalized Advertising, and Privacy Controls. *Journal of Marketing Research*, 51(5), 546, 546–562.
- Van Doorn, J. & Hoekstra, J. C. (2013). Customization of Online Advertising: the Role of Intrusiveness. *Marketing Letters*, 24(4), 339–351. <http://doi.org/10.1007/s11002-012-9222-1>
- Verlegh, P. W. J., Franssen, M. L. & Kirmani, A. (n.d.). *International Journal of Advertising : the Review of Marketing Communications Persuasion in Advertising: When Does It Work, and When Does It Not ?* (February 2015), 37–41.
<http://doi.org/10.1080/02650487.2014.994732>
- Wells, J., Valacich, J. & Hess, T. (2011). What Signals Are You Sending? How Website Quality Influences Perceptions of Product Quality and Purchase Intentions. *MIS Quarterly*, 35(2), 373–396. Retrieved from
<http://uedi.dongguk.edu/files/2012041818424619.pdf\npapers3://publication/uuid/1C8ED71C-BDD1-4B43-8EDC-43DADC85C569>
- Westlund, O., Gómez-Barroso, J.-L., Compañó, R. & Feijóo, C. (2011). Exploring the Logic of Mobile Search. *Behaviour & Information Technology*, 30(5), 691–703.
<http://doi.org/10.1080/0144929X.2010.516020>
- White, T. B., & Yuan, H. (2012). Building trust to increase purchase intentions: The signaling impact of low pricing policies. *Journal of Consumer Psychology*, 22(3), 384-394. <http://doi.org/10.1016/j.jcps.2011.09.003>
- 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.
<http://doi.org/10.1016/j.dss.2010.11.017>


Xu, H., Teo, H. H., Tan, B. C. Y. & Agarwal, R. (2012a). Effects of Individual Self-Protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: a Study of Location-based Services. *Information Systems Research*, 23(4), 1342–1363. <http://doi.org/10.1287/isre.1120.0416>

Xu, H., Teo, H. H., Tan, B. C. Y. & Agarwal, R. (2012b). Effects of Individual Self-Protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: a Study of Location-based Services. *Information Systems Research*, 23(4), 1342–1363. <http://doi.org/10.1287/isre.1120.0416>


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

APPENDICES

APPENDIX A - E-MAIL ADVERTISEMENT GROUP A



"Get the hound to sniff around"



**KNOW
WHAT YOU'RE
PAYING FOR**

GET MEDICAL COVER QUOTES

Secured site

Dear {firstname}

Some of us get the occasional sniffles once per year, while others make regular trips to the doctor and become familiar with the world of wards. Either way, the loyal [iHound](#) is there to make sure you're covered. But is it a hospital plan or comprehensive medical aid that you need? iHound sniffed out a few differences to help you make the best decision.

What are you paying for?

If you've signed up for a hospital plan, you're only paying for medical care in hospital. That doesn't necessarily include any medication or treatment out of or after a stay in hospital.

A comprehensive medical aid will pay for your treatment both in and out of hospital whether you're staying the night or not. A number of chronic diseases and other conditions are also covered by medical aid.


What's the best option?

The choice is all yours, but consider that medical aid often includes additional benefits such as maternity care, trips to the dentist and the optometrist, which hospital plans don't include. Even if you hardly ever visit the doctor yourself, you'll need to send your kids for regular checkups to ensure their teeth and eyes are taken care of. Ask iHound to sniff out a few [quotes](#) for you to compare and get the best medical care you can afford.


The iHound Team

To opt out from this mailing list, you can [{UNSUBSCRIBEHYPERLINK}](#)

APPENDIX B - E-MAIL ADVERTISEMENT GROUP B



"Get the hound to sniff around"



Dear {firstname}

Some of us get the occasional sniffles once per year, while others make regular trips to the doctor and become familiar with the world of wards. Either way, the loyal [iHound](#) is there to make sure you're covered. But is it a hospital plan or comprehensive medical aid that you need? iHound sniffed out a few differences to help you make the best decision.

What are you paying for?

If you've signed up for a hospital plan, you're only paying for medical care in hospital. That doesn't necessarily include any medication or treatment out of or after a stay in hospital.

A comprehensive medical aid will pay for your treatment both in and out of hospital whether you're staying the night or not. A number of chronic diseases and other conditions are also covered by medical aid.

What's the best option?

The choice is all yours, but consider that medical aid often includes additional benefits such as maternity care, trips to the dentist and the optometrist, which hospital plans don't include. Even if you hardly ever visit the doctor yourself, you'll need to send your kids for regular checkups to ensure their teeth and eyes are taken care of. Ask iHound to sniff out a few [quotes](#) for you to compare and get the best medical care you can afford.

The iHound Team

To opt out from this mailing list, you can [UNSUBSCRIBE\(HYPERLINK\)](#).

APPENDIX C - GROUP A AND B WEBSITE

The screenshot displays the iHound website interface. At the top, the browser address bar shows 'insurancehound.co.za'. The website header features the iHound logo with a dog icon and the tagline 'Get the hound to sniff around', along with social media icons for Facebook, Twitter, and Google+. The main content area is split into two columns. The left column is titled 'Comprehensive Medical Aid Quotes!' and features a photograph of four medical professionals. Below the photo, the text describes the service: 'Medical Insurance' and 'Benefits'. The right column is titled 'Get Quotes and Save!' and contains a registration form with fields for Name, Surname, Email, Cell Number, Province, and Monthly Gross Income. A checkbox for 'I agree to the website terms & conditions' is checked, and a red 'Get Quotes >' button is prominent. Below the button is a 'Secured site' icon. The footer contains a navigation menu with links for Car Insurance, Business Insurance, Life Insurance, Motor Warranty, Medical Aid, Funeral Insurance, Legal Insurance, Hospital Insurance, and Home Insurance. It also includes an 'About Us' section with links for Affiliate Programme, Articles, Insurance Quotes, Brokers, Suppliers, and Terms & Conditions. The copyright notice at the bottom reads: 'Copyright © iHound - All Rights Reserved. Physical Address: 100A Frances Road, Norwood, Johannesburg, 2192'.

APPENDIX D – ETHICAL CLEARANCE APPROVAL

**Gordon Institute
of Business Science**
University of Pretoria

Dear Lee Zuk

Protocol Number: **Temp2015-01689**

Title: Examining the influence of a privacy symbol within an e-mail advert, on a consumer's behaviour around their disclosure of private information.

Please be advised that your application for Ethical Clearance has been APPROVED.

You are therefore allowed to continue collecting your data.

We wish you everything of the best for the rest of the project.

Kind Regards,

Adele Bekker

APPENDIX E – TURNITIN REPORT



Will the use of a third-party privacy seal (lock) in an e-mail advertisements result in a higher likelihood of consumers disclosing their private information? by Lee Zuk

From Test your originality (GIBS Information Center)

- Processed on 06-Nov-2015 16:50 SAST
- ID: 596322980
- Word Count: 24303

Similarity Index

14%

Similarity by Source

Internet Sources:

9%

Publications:

7%

Student Papers:

10%

sources:

1% match (Internet from 26-Aug-2003)	1
http://www.girlsru.com/swimsuit-photos/	
1% match (Internet from 03-Sep-2015)	2
http://scholar.sun.ac.za/bitstream/handle/10019.1/4787/benade_critical_2009.pdf?sequence=1	
< 1% match (student papers from 11-Sep-2014)	3
Submitted to University of Wales, Bangor on 2014-09-11	
< 1% match (Internet from 20-Feb-2014)	4
http://pal.ist.psu.edu/MISQ.pdf	

5

< 1% match (student papers from 02-Sep-2015)

[Submitted to Appalachian State University on 2015-09-02](#)

6

< 1% match (publications)

[John, Leslie K., Alessandro Acquisti, and George Loewenstein. "Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information", Journal of Consumer Research, 2011.](#)

7

< 1% match (student papers from 20-Oct-2015)

[Submitted to Laureate Higher Education Group on 2015-10-20](#)

8

< 1% match (Internet from 10-Nov-2014)

[http://upetd.up.ac.za/thesis/available/etd-07212012-171424/unrestricted/dissertation.pdf](#)

9

< 1% match (student papers from 30-Oct-2012)

[Submitted to University of Pretoria on 2012-10-30](#)

10

< 1% match (Internet from 28-Oct-2015)

[http://www.airitilibrary.com/Publication/alDetailedMesh1?DocID=U0001-2706201414401700](#)

11

< 1% match (student papers from 11-Sep-2014)

[Submitted to University of Northumbria at Newcastle on 2014-09-11](#)

12

< 1% match (publications)

[Xu, H., H.-H. Teo, B. C. Y. Tan, and R. Agarwal. "Research Note--Effects of Individual Self-Protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: A Study of Location-Based Services", Information Systems Research, 2012.](#)

13

< 1% match (Internet from 03-May-2014)

[http://upetd.up.ac.za/thesis/available/etd-04032011-154248/unrestricted/dissertation.pdf](#)

14

< 1% match (Internet from 18-Nov-2013)

[http://www.rebeccahunt.com/academic/index.html](#)

15

< 1% match (student papers from 28-Aug-2015)

[Submitted to Goldsmiths' College on 2015-08-28](#)

16

< 1% match (publications)

[Yue-Teng Wong; Osman, Syuhaily; Said, Aini and Paim, Laily. "Moderating Effect of Gender in Repatronage Behavioral Intention: The Role of Personal Characteristics", Asian Social Science, 2014.](#)

17

< 1% match (student papers from 02-Sep-2015)

[Submitted to University of Northumbria at Newcastle on 2015-09-02](#)

18

< 1% match (student papers from 26-Dec-2014)

[Submitted to Bridgepoint Education on 2014-12-26](#)

19

< 1% match (student papers from 29-Feb-2012)

[Submitted to Southern New Hampshire University - Continuing Education on 2012-02-29](#)

20

< 1% match (publications)

["Study results from I. Sekine and colleagues in the area of non-small cell lung cancer published.", Cancer Weekly, May 19 2009 Issue](#)

21

< 1% match (Internet from 23-Nov-2011)

<http://www.rotman.utoronto.ca/~agoldfarb/GoldfarbTucker-intrusiveness.pdf>

22

< 1% match (student papers from 19-Apr-2015)

[Submitted to Laureate Higher Education Group on 2015-04-19](#)

23

< 1% match (student papers from 25-Jul-2015)

[Submitted to University of Maryland, University College on 2015-07-25](#)

24

< 1% match (Internet from 01-Dec-2011)

<http://www.misq.org/skin/frontend/default/misq/pdf/V35I4/PavlouIntroduction.pdf>

25

< 1% match (student papers from 27-Aug-2015)

[Submitted to King's College on 2015-08-27](#)

26

< 1% match (student papers from 22-May-2015)

[Submitted to University of Portsmouth on 2015-05-22](#)

27

< 1% match (student papers from 05-Mar-2013)

Submitted to American Intercontinental University Online on 2013-03-05

28

< 1% match (student papers from 26-Jul-2013)

Submitted to University of Newcastle on 2013-07-26

29

< 1% match (publications)

Keith, Mark J., Samuel C. Thompson, Joanne Hale, Paul Benjamin Lowry, and Chapman Greer. "Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior", International Journal of Human-Computer Studies, 2013.

30

< 1% match (publications)

Spiekermann, Sarah, Alessandro Acquisti, Rainer Böhme, and Kai-Lung Hui. "The challenges of personal data markets and privacy", Electronic Markets, 2015.

31

< 1% match (publications)

"Local Leaders Join Edelman CEO to Discuss the Role of Trust in Innovation.", PR Newswire, March 12 2015 Issue

32

< 1% match (Internet from 04-May-2013)

<http://www.euractiv.com/de/innovation-enterprise/werbung-und-verbraucherrechte-linksdossier-189306>

33

< 1% match (publications)

Mothersbaugh, D. L., W. K. Foxx, S. E. Beatty, and S. Wang. "Disclosure Antecedents in an Online Service Context: The Role of Sensitivity of Information", Journal of Service Research, 2012.

34

< 1% match (student papers from 27-Aug-2015)

Submitted to University of Warwick on 2015-08-27

35

< 1% match (publications)

Turnitin DB,

36

< 1% match (Internet from 28-Jun-2012)

<http://www.thinking-and-reasoning-arena.com/common/sample-chapters/9781848728523.pdf>

37

< 1% match (publications)

[Knijnenburg, Bart P., and Alfred Kobsa. "Making Decisions about Privacy : Information Disclosure in Context-Aware Recommender Systems", ACM Transactions on Interactive Intelligent Systems, 2013.](#)

38

< 1% match (student papers from 02-Mar-2015)

[Submitted to University of Queensland on 2015-03-02](#)

39

< 1% match (student papers from 17-Sep-2007)

[Submitted to Royal Holloway and Bedford New College on 2007-09-17](#)

40

< 1% match (student papers from 02-Sep-2013)

[Submitted to University of Exeter on 2013-09-02](#)

41

< 1% match (Internet from 28-Oct-2015)

http://www.researchgate.net/publication/279069334_Location_information_disclosure_in_location-based_social_network_services_Privacy_calculus_benefit_structure_and_gender_differences

42

< 1% match (Internet from 29-Oct-2015)

<http://c000-crown-of-thorns-abc.net.au/news/2014-04-22/new-method-kills-more-than-2502c000-crown-of-thorns->

43

< 1% match (Internet from 16-Mar-2009)

http://www.accessmylibrary.com/coms2/summary_0286-141080_ITM

44

< 1% match (publications)

[Mavlanova, Tamilla, Raquel Benbunan-Fich, and Marios Koufaris. "Signaling theory and information asymmetry in online commerce", Information & Management, 2012.](#)

45

< 1% match (student papers from 03-Jul-2013)

[Submitted to CUNY, Hunter College on 2013-07-03](#)

46

< 1% match (student papers from 27-Oct-2014)

[Submitted to Bournemouth University on 2014-10-27](#)

47

< 1% match (publications)

[Bonsón Ponte, Enrique, Elena Carvajal-Trujillo, and Tomás Escobar-Rodríguez. "Influence of](#)

[trust and perceived value on the intention to purchase travel online: Integrating the effects of assurance on trust antecedents", Tourism Management, 2015.](#)

48

< 1% match (student papers from 04-Sep-2015)

[Submitted to Nottingham Trent University on 2015-09-04](#)

49

< 1% match (publications)

[Westlund, Oscar and Färdigh, Mathias A.. "Conceptualizing Media Generations: The Print, Online and Individualized Generations", Observatorio \(OBS*\), 2012.](#)

50

< 1% match (Internet from 05-Apr-2013)

<http://www.heinz.cmu.edu/~acquisti/papers/acquisti-privacy-worth.pdf>

51

< 1% match (publications)

[Mukherjee, Partha, and Bernard J. Jansen. "Gender-brand effect of search queries on sponsored search performance : Gender-Brand Effect of Search Queries on Sponsored Search Performance", Proceedings of the American Society for Information Science and Technology, 2013.](#)

52

< 1% match (student papers from 31-Mar-2012)

[Submitted to University of Maryland, University College on 2012-03-31](#)

53

< 1% match (student papers from 05-Jun-2015)

[Submitted to Southern New Hampshire University - Distance Education on 2015-06-05](#)

54

< 1% match (Internet from 06-Sep-2014)

http://www.doria.fi/bitstream/handle/10024/98716/Ae8_2014.pdf?sequence=2

55

< 1% match (Internet from 28-Apr-2013)

http://iamireland.ie/wp-content/uploads/2013/02/IJM-312-2012-Final_crop.pdf

56

< 1% match (publications)

[Finch, James. "Managerial Marketing", Bridge Point, 2012.](#)

57

< 1% match (student papers from 16-Dec-2004)

[Submitted to Massey University on 2004-12-16](#)

58

< 1% match (Internet from 05-Jun-2015)

http://repository.up.ac.za/bitstream/handle/2263/40760/Molefe_Data_2013.pdf?sequence

59

< 1% match (student papers from 20-Aug-2015)

[Submitted to Kingston University on 2015-08-20](#)

60

< 1% match (Internet from 25-May-2014)

<http://repository.up.ac.za/bitstream/handle/2263/29623/dissertation.pdf?sequence=1>

61

< 1% match (Internet from 20-May-2012)

http://sprouts.aisnet.org/1167/1/JAIS-TDW-2011_001.pdf

62

< 1% match (Internet from 18-Jun-2013)

<http://www.annehelmond.nl/page/9/>

63

< 1% match (student papers from 31-Aug-2015)

[Submitted to University of Sheffield on 2015-08-31](#)

64

< 1% match (student papers from 18-Jan-2013)

[Submitted to Cranfield University on 2013-01-18](#)

65

< 1% match (Internet from 27-Dec-2014)

http://www.pacis2014.org/data/PACIS_mainconference/pdf/pacis2014_submission_386.pdf

66

< 1% match (Internet from 11-May-2015)

http://repository.up.ac.za/bitstream/handle/2263/40645/Stirling_Practices_2013.pdf?sequ

67

< 1% match (Internet from 07-Mar-2014)

<http://www.repository.up.ac.za/bitstream/handle/2263/23470/dissertation.pdf?se>

68

< 1% match (Internet from 04-May-2011)

<http://www.grainsa.co.za/documents/1%20Jul%20Bio-ethanol.pdf>

69

< 1% match (Internet from 11-Oct-2010)

http://www.bridging.uwaterloo.ca/uwcisa/symposiums/symposium_2005/No%20et%20al.pdf

70

< 1% match (Internet from 06-Feb-2014)

http://pefprints.pef.uni-lj.si/1633/1/Diploma%2DOsterman_Petra.pdf

71

< 1% match (student papers from 24-Apr-2015)

[Submitted to University of Huddersfield on 2015-04-24](#)

72

< 1% match (Internet from 16-Apr-2014)

<http://upetd.up.ac.za/thesis/available/etd-04042011-185539/unrestricted/dissertation.pdf>

73

< 1% match (Internet from 21-Apr-2013)

<http://www.palgrave-journals.com/ejis/journal/v21/n6/full/ejis201213a.html>

74

< 1% match (Internet from 12-Jun-2015)

<http://saisconferencemgmt.org/proceedings/2014/Rusk.pdf>

75

< 1% match (publications)

["ThisIsMe, a solution to online fraud and identity theft in South Africa.", Bizcommunity.com, March 3 2015 Issue](#)

76

< 1% match (Internet from 29-Jun-2015)

<http://repository.up.ac.za/bitstream/handle/2263/24251/dissertation.pdf?sequence>

77

< 1% match (publications)

[van Baal, Sebastian. "Not all seals are equal: An experimental investigation of the effect of third-party seals on purchase probability in electronic commerce", Electronic Commerce Research, 2015.](#)

78

< 1% match (publications)

["Hydes of Norwich Extends Its Reach Beyond Norfolk With The Launch Of A New Ecommerce Website.\(Websit", ICT Monitor Worldwide, Oct 29 2015 Issue](#)

79

< 1% match (student papers from 31-Oct-2012)

[Submitted to University of Pretoria on 2012-10-31](#)

80

< 1% match (Internet from 18-Jan-2015)

<http://repository.up.ac.za/bitstream/handle/2263/23459/dissertation.pdf?sequence=1>

81

< 1% match (Internet from 18-Jan-2015)

<http://house.gov/>

82

< 1% match (publications)

[Faqih, Khaled M. S., and Mohammed-Issa Riad Jaradat. "Mobile Healthcare Adoption among Patients in a Developing Country Environment: Exploring the Influence of Age and Gender Differences", International Business Research, 2015.](#)

83

< 1% match (publications)

[Asian Review of Accounting, Volume 22, Issue 3 \(2014-09-16\)](#)

84

< 1% match (student papers from 01-Nov-2011)

[Submitted to University of Pretoria on 2011-11-01](#)

85

< 1% match (student papers from 22-Aug-2015)

[Submitted to Waterford Institute of Technology on 2015-08-22](#)

86

< 1% match (student papers from 05-Aug-2014)

[Submitted to Bournemouth University on 2014-08-05](#)

87

< 1% match (publications)

[Roeber, Bjoern, Olaf Rehse, Robert Knorrek, and Benjamin Thomsen. "Personal data: how context shapes consumers' data sharing with organizations from various sectors", Electronic Markets, 2015.](#)

88

< 1% match (Internet from 15-Apr-2014)

<http://upetd.up.ac.za/thesis/available/etd-04032011-131147/unrestricted/dissertation.pdf>

89

< 1% match (Internet from 19-Apr-2015)

http://repository.up.ac.za/bitstream/handle/2263/40181/Harmse_South_2013.pdf?sequence=1

90

< 1% match (Internet from 21-Sep-2015)

<http://repository.up.ac.za/bitstream/handle/2263/23765/dissertation.pdf?sequence=1>

91

< 1% match (Internet from 17-Jun-2015)

<http://repository.up.ac.za/bitstream/handle/2263/24400/dissertation.pdf?sequence=1&isAllow>

92

< 1% match (Internet from 08-Sep-2014)

<http://upetd.up.ac.za/thesis/available/etd-08042012-201732/unrestricted/dissertation.pdf>

93

< 1% match (Internet from 18-May-2014)

<http://upetd.up.ac.za/thesis/available/etd-05052010-153654/unrestricted/dissertation.pdf>

94

< 1% match (Internet from 12-Jan-2014)

<http://www.aeaweb.org/aea/2014conference/program/retrieve.php?pdfid=151>

95

< 1% match (Internet from 19-Sep-2014)

<http://simson.net/work/hcisec-review.pdf>

96

< 1% match (Internet from 10-Jun-2013)

http://faculty.ist.psu.edu/jjansen/academic/jansen_gender_ppc.pdf

97

< 1% match (publications)

[Kehr, Flavius, Tobias Kowatsch, Daniel Wentzel, and Elgar Fleisch. "Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus : Privacy calculus: dispositions and affect", Information Systems Journal, 2015.](#)

98

< 1% match (publications)

[Developments in Marketing Science Proceedings of the Academy of Marketing Science, 2015.](#)

99

< 1% match (publications)

[Libaque-Saenz, C. F., S. F. Wong, Y. Chang, Y. W. Ha, and M.-C. Park. "Understanding antecedents to perceived information risks: An empirical study of the Korean telecommunications market", Information Development, 2014.](#)

100

< 1% match (student papers from 24-May-2012)

[Submitted to London School of Economics and Political Science on 2012-05-24](#)

101

< 1% match (Internet from 03-Jun-2015)

<http://repository.up.ac.za/bitstream/handle/2263/23865/dissertation.pdf?sequence=1>

102

< 1% match (Internet from 08-Feb-2014)

<http://swissim.com/wp-content/uploads/2011/11/Paper-Directors-Dealings-as-an-Investment-Indicator.pdf>

103

< 1% match (Internet from 02-Sep-2015)

<http://repository.up.ac.za/bitstream/handle/2263/26828/dissertation.pdf?sequence=1>

104

< 1% match (Internet from 22-Dec-2009)

http://theses.nps.navy.mil/04Jun_Hakola.pdf

105

< 1% match (Internet from 29-Aug-2011)

<http://www.entrepreneur.com/tradejournals/article/163394870.html>

106

< 1% match (Internet from 15-May-2012)

[http://www.cspforum.eu/uploads/monetising_privacy_\(1\).pdf](http://www.cspforum.eu/uploads/monetising_privacy_(1).pdf)

107

< 1% match (Internet from 05-Apr-2011)

<http://onlinelibrary.wiley.com/doi/10.1111/j.1745-6606.2002.tb00419.x/abstract>

108

< 1% match (publications)

[Industrial Management & Data Systems, Volume 111, Issue 2 \(2011-03-06\)](#)

109

< 1% match (publications)

[Paul Benjamin Lowry. "Using an elaboration likelihood approach to better understand the persuasiveness of website privacy assurance cues for online consumers", Journal of the American Society for Information Science and Technology, 04/2012](#)

110

< 1% match (publications)

[Niepmann, Friederike. "Bank Bailouts, International Linkages and Cooperation", Working Papers \(Oesterreichische Nationalbank\), 20110524](#)

111

< 1% match (publications)

[Wright, Ryan, and David Wilson. "Privacy, Accuracy and Accessibility of Digital Business", Computing Handbook Third Edition, 2014.](#)

112

< 1% match (publications)

[Treiblmaier, Horst Chong, Sandy. "Trust and perceived risk of personal information as antecedents of online information disclosure: re", Journal of Global Information Management, Oct-Dec 2011 Issue](#)

paper text:

Will the use of a third-party privacy seal (lock) in an e-mail advertisements result in a higher likelihood of consumers disclosing their private information? Lee Zuk 14448166

9A

research proposal submitted to the Gordon Institute of Business Science,

University of Pretoria, in partial fulfilment of the requirements of the degree

of Master of Business Administration. 09 November 2015 **ABSTRACT** One

of the commodities in the commercial world has become access to data, specifically

personal information. The Internet has rapidly expanded a company's ability to access consumers' and individuals' personal information, however consumers' privacy-concerns regarding the disclosure of their personal information have continued to increase. Using an e-mail marketing campaign, this research explored the impact of using third-party privacy seal (lock) as signals to facilitate consumers disclosing private information. The study employed a live experimental randomised two-group post-test only design, whereby an e-mail advertisement, identical in design except for the image of a third party seal (lock) placed on the non-control group's e-mail. The test explored whether the e-mail advertisement containing the third-party privacy signal (lock) had an impact on whether or not the recipient behaved in a certain way in comparison to the e-mail advertisement that did not contain a lock. The results showed no real significant difference of the third-party seal (lock) on the consumer's preparedness to disclose personal information. Whilst the lock may be used as a trust symbol it is not enough, within the online advertising context, to entice disclosure of personal information. To remain competitive, companies will need to reassess their advertising strategies and further research will need to identify high value signals to encourage consumer disclosure. Keywords Privacy, consumer disclosure, online advertising,