



Privacy in the Digital Age: Understanding the Effects of Privacy Invasion on South African Consumers' Brand Trust

By

Elke Stegmann | [REDACTED]

A research report submitted in fulfilment of the requirements for the BCom Honours in Strategic Brand Management at the Independent Institute of Education: Vega School.

Supervisor: Dr Tish Taylor

Module: Research

Module Code: RESE8419w

Qualification: BCom Honours in Strategic Brand Management

Submission Date: 20 November 2023.

Word Count: 11 853

Declaration:

I hereby declare that the Research Report submitted for the BCom Honours in Strategic Brand Management degree to The Independent Institute of Education is my own work and has not previously been submitted to another University or Higher Education Institution for degree purposes.

[REDACTED]

Abstract

With the advancements in data-gathering technology, various privacy-related issues such as a lack of consumer knowledge about data gathering and protection, lack of regulation, and a decrease in trust from consumers toward brands and digital marketing have arisen. Despite an increase in data-related research there remains a methodological gap in the literature with much of the existing research approaching the topic quantitatively. This study aimed at understanding how consumers are affected by invasive digital marketing activities, and how this affects their trust in brands, specifically in the context of South African consumers. Utilising a qualitative research design and inductive reasoning techniques participants were sampled using snowball and purposive sampling techniques. The data was collected using an in-depth interview and analysed through narrative analysis. The findings indicated that all participants had experienced some form of privacy invasion driven by digital marketing and brands in the online space. This in turn had a negative impact on their brand trust and overall view of digital marketing. However, many participants saw the necessity of online information sharing with brands and had various recommendations and thoughts on how trust could be regained. Based on the data, several recommendations can be made; brands should be as transparent as possible regarding their data gathering and processing practices, brands should at least meet, and preferably go beyond privacy regulations and expectations, and consumers should make an effort to educate themselves on digital privacy and how their data is collected, processed, and shared.

Keywords: brand trust, data privacy, digital privacy, privacy invasion, digital marketing.

Table of Contents

Abstract	1
Introduction	1
Contextualisation	1
Rationale	1
Problem Statement	2
Purpose Statement	2
Research Question	3
Research Objectives	3
Literature Review	4
Conceptualisation	4
Personal Information/Data	4
Data Governance & Data Protection	4
Privacy Violation	5
Marketing Technology	5
Theoretical Foundation	6
Privacy	6
Brand Trust	8
Literature Review	9
Ways Consumer Privacy is Affected	9
Attitude of Consumers	11
Consumer Control Over Personal Data	12
Effect Of Invasive Marketing Practices	13
How Brands Can Solve Privacy Problems	15
Conclusion	16
Research Design & Methodology	17
Research Paradigm	17
Ontological Position	18
Epistemological Position	18
Axiological Position	18
Research Design and Approach	19

Research Design	19
Type of Reasoning:	19
Type of Research:	20
Time-Dimension:	20
Population	20
Sampling.....	21
Data Collection	22
Data Analysis	23
<i>Findings & Interpretation of Findings.....</i>	<i>25</i>
Addressing The Research Question, Problem, and Objectives	32
Questions	32
Problem	33
Objectives.....	34
<i>Conclusion.....</i>	<i>36</i>
Trustworthiness	36
Anticipated Contribution.....	36
Ethical Consideration	37
Limitations.....	37
<i>Reference List.....</i>	<i>38</i>
<i>Annexure A: Example of Consent Forms.....</i>	<i>45</i>
Participant Consent Form	45
Audio or Video Recording Consent Form.....	47
Quantitative Disclaimer.....	48
<i>Annexure B: Measurement Instruments.....</i>	<i>49</i>
<i>Annexure C: Ethical Clearance Letter</i>	<i>51</i>
<i>Annexure D: Concept Document</i>	<i>52</i>
<i>Annexure E: Research Questions.....</i>	<i>55</i>

Introduction

Contextualisation

“Privacy is one of the most critical issues of our time.” (Turrecha & Ashley, 2021:5)

Acquiring consumer information is crucial to organisations operating in a highly digitised world and business environment (Engels, 2019). Data gathering and marketing technology advancements have transformed consumer information collection, analysis, and storage. These technological advancements have far outpaced privacy-protecting regulations and organisational responsibility concerning consumer privacy – resulting in consumers losing power over their data and consequently, their privacy (Bandara, Fernando, & Akter, 2020). Digital marketing requires extensive information on consumers to be successful. This has led to ethically questionable data gathering and analysis techniques being utilised in some cases (Martin & Murphy, 2017).

According to Yuvaraj and Indumathi (2018), digital marketing is crucial to successful brand building in the modern world. Digital marketing supports brand communication, loyalty, recognition and more (Yuvaraj & Indumathi, 2018). Digital marketing can be considered an extension of a brand which is why it has an impact on brand trust. This study will explore how invasive – or perceived invasive digital marketing activities – affect consumers’ experience with and trust in a brand. This study can be used by marketing and branding professionals interested in the ethical use of consumer data.

In the sections that follow, a compelling argument as to why this topic should be researched is presented. This study follows a qualitative approach. The literature review creates a clear understanding of relevant theories namely, privacy and brand trust theories and supporting concepts. Followed by an in-depth discussion of invasive digital marketing techniques and consumers’ experience with them. This provides sufficient insights from previous literature as to why this topic is worth researching. What follows is a breakdown of the research, creating a clear and realistic roadmap for this study. Finally, a reflection on the limitations, contributions, and ethical considerations of this study is given.

Rationale

Ashworth and Free (2006) state that digital marketing technology has and continues to evolve at a rapid pace, and with it, privacy concerns grow. According to Martin & Murphy

(2017), relevant academic materials have not evolved as rapidly as marketing technology and marketers' use of consumer data, limiting the reliable information that is available on the topic. This rapid development of marketing technology combined with the need for highly detailed and personal consumer information to be successful has led to unfair and in some instances even aggressive data-gathering and digital marketing techniques that result in customer suspicion and frustration (Mandal, 2019). Additionally, consumers feel ill-equipped to regain or stay in control of their personal information due to a lack of knowledge regarding the technology and complex privacy policies (Albulayhi & Khediri, 2022). Wang (2018) found that consumers' privacy concerns regarding digital marketing had a predominantly negative effect on their trust in brands which ultimately had a negative impact on the consumer-brand relationship. There is a gap in the understanding of the effects data gathering and loss of ownership over data have on consumers' trust in and relationships with brands. This study aims to lessen that gap by shedding light on the technology and practices that are truly invasive, how consumers are affected by this invasion, and how their trust is consequently affected.

Problem Statement

Massive amounts of consumer data are collected, analysed, and stored for digital marketing purposes (Wang & Baker, 2022), frequently without the consumer's full awareness or understanding (Martin & Murphy, 2017). This has diminished the understanding of and respect for digital privacy and the violation thereof. Yuvaraj and Indumathi (2018) state that digital marketing activities are an extension of brand building, which means that any feelings consumers have towards digital marketing activities, will be transferred to the brand as well. Additionally, Kelly, Kerr, and Drennan (2017) found that consumers' trust in brands has decreased in the digital space due to the reasons stated above. Kelly *et al.* (2017) state that consumers have more trust in technology than they do in the brands communicating with them using this technology. The problem is that consumers are being affected by unethical digital marketing activities and that possibly hurts brand trust.

Purpose Statement

The purpose of this study is to understand how consumers are affected by invasive data gathering techniques – specifically for digital marketing purposes – and how this has impacted their trust in and relationship with brands.

Research Question

Primary:

1. How does online data gathering, driven by digital marketing activities, impact on consumer relationships and brand trust?

Secondary:

2. When do consumers perceive data gathering to be an invasion of digital privacy?
3. How is the success of digital marketing and online brands impacted by this experience with privacy invasion?
4. How is the control of consumers over their information affected by digital marketing activities?
5. How does the experience of consumers affect their trust in and relationships with brands?

Research Objectives

1. Determine which digital marketing activities affect consumer privacy.
2. Understand the attitude of consumers towards these digital marketing activities.
3. Determine how much control consumers have or had over their data.
4. Determine how organisations can help minimise or solve privacy concerns.
5. Understand how invasive data gathering affects South African consumers' trust in and relationship with brands.

Literature Review

Conceptualisation

There are 4 key concepts in this research project:

Personal Information/Data

Wahyuningtyas (2017) defines personal data as information defining a person through physical, psychological, genetic, or societal factors. Martin and Murphy (2017) define personal data as information belonging to an individual which is theirs alone to share.

This research project is concerned with consumers' personal data and how it is or can be affected by digital marketing activities and data gathering. This concept relates to the following theories of privacy:

Privacy as control. How much control do consumers have over who has access to their personal information?

Privacy as power. If an individual has control of their personal information, they have power. Alternatively, if an organisation has control over their information, it has power.

Privacy as obscurity. If the consumer in question's information is easily accessible and understandable, they cannot obscure it.

Data Governance & Data Protection

Data governance is an agreed-upon organisational model that defines who has the right to act on information, in which context it occurs, how it occurs, and with what methods it occurs (Turrecha & Ashley, 2021). This goes hand in hand with data protection which refers to how an organisation protects the information they own and acquire, it is the process of respecting and adhering to a person's privacy preferences (Turrecha & Ashley, 2021). These concepts are relevant to consumers' control over their personal information, and how brands can improve privacy-related issues. This concept is related to the theory of privacy as trust. Consumers should be able to trust that brands have data governance models in place and will protect their data to the best of their abilities. This study will consider the role brands play in solving or preventing privacy problems, this is where the concept of data governance becomes very relevant.

Privacy Violation

Privacy violation can be conceptualised using Daniel Solove's pragmatic view of privacy. Solove, as cited by Zeccherini (2015) looks at the context within which privacy has been or can be violated. He suggests four categories of privacy violation: invasion, collection, processing, and dissemination (Zeccherini, 2015). This is a suitable conceptualisation as the collection, processing and dissemination of information all fall under digital marketing's, use of data – made evident by the definitions in Table 1. It can be deduced that if any of the categories are negatively affected, privacy has been violated. This concept will also be of value in the data collection process. The four categories of privacy violation will provide valuable context for me as the researcher and interview participants to truly understand the context the participant's privacy was violated.

Marketing Technology

Marketing Technology (Martech) is software solutions that support digital marketing activities and innovation (Turrecha & Ashley, 2021). Martech is used in advertising, direct marketing, content creation, customer experience, data and analytics, and user experience (Turrecha & Ashley, 2021). The technology has led to process automation, advanced monitoring and processing of data and information, and other highly valuable processes (Turrecha & Ashley, 2021). Another dimension of martech is ad technology (ad tech) which incorporates analytical tools such as AI, machine learning or Big Data, and technical tools used to gather extensive information on consumers - these technologies have been under global scrutiny and their success has been disrupted thanks to developments in privacy technology such as the ability to block third-party cookies and new privacy legislation (Turrecha & Ashley, 2021). One such legislation is South Africa's Protection of Personal Information Act (PoPIA or PoPI Act) which aims to safeguard South African citizens' privacy and information by ensuring organisations, companies, and any individual that possesses and handles personal data in South Africa adheres to certain conditions and principles surrounding the possession and handling of the data (Breaker-Rolfe, 2023). In the literature review, Martech software that poses a threat to digital privacy is discussed in detail. It is important to comprehend the meaning of Martech and understand precisely which software can or does violate consumer privacy as it is a driver of privacy concerns within digital marketing it is one of the reasons invasive practices came to be – making it a key concept of this research project.

Theoretical Foundation

There are 2 theories underlying this study namely, privacy and brand trust.

Privacy

Several authors, philosophers, and thought leaders have attempted to define and conceptualise privacy. However, the multi-faceted nature of privacy has resulted in no one definition being universally accepted as true. Within the rapidly evolving digital landscape, privacy becomes even more fluctuant – the result is that protecting privacy, particularly online, is not understood or enforced by consumers or brands. For this reason, a multi-definition approach to defining and theorising privacy will be taken in this study.

Privacy as Control

First conceptualised by Alan Westin, this definition focuses on how much control an individual has over how much of their personal information is shared, with whom, how, and when it is shared (Rollenhagen, 2020). This definition was first conceptualised in 1967 before the internet or digital privacy was of consideration (Rollenhagen, 2020). However, it remains relevant today, and to this study, as the ability to control one's information is applicable online and offline. It is useful to look at privacy as control within two dimensions defined by Ashworth and Free (2006) the first being aware of data collection, and the second being the usage of information. Awareness means a consumer is aware their data is being accessed while usage refers to the way digital marketers use the information (Ashworth & Free, 2006). If consumers are unaware of how their data is collected or used, there is a lack of control. These dimensions are further discussed in the literature review section – consumer control over personal data. Control is an important aspect in the case of digital privacy. If consumers lack complete control, it can be argued that they never possessed any privacy in the digital landscape.

Privacy as Obscurity

Selinger and Hartzog (2014) define privacy as obscurity – one's personal information is private if it's difficult for others to access or understand it. The authors elaborate by stating that when information is difficult to obtain only an extremely motivated person or entity will search for it and attempt to understand it (Selinger & Hartzog, 2014). Obscuring personal information is becoming increasingly difficult in the digital age where technologies such as big data and artificial intelligence (AI) are transforming the way information is gathered and analysed – meaning even if consumers attempt to obscure information, marketers can still

access it using advanced technologies. A more in-depth look at these technologies and their use in digital marketing is provided in the literature review. Selinger and Hartzog (2014) go on to outline certain ways that obscurity, specifically in the digital space, can be maintained, despite the advancements in technology. These include but are not limited to using privacy settings, using a pseudonym, and codifying information one discloses online (Selinger & Hartzog, 2014). This study aims to determine to what extent consumers can obscure information if they try at all. It will also consider to what extent privacy was truly violated if no effort to obscure information was made.

Privacy as Trust

Waldman (2015) defines privacy as a social construct formed around trust. In this case, trust refers to the expectation that others' behaviour will not have a negative impact on you (Waldman, 2015). Richards and Hartzog (2017) go on to say trust refers to one's readiness to share information with others. Trust between an individual and organisations can be built through sustainable and ethical privacy policies, regulations, and laws (Richard & Hartzog, 2017). The PoPI Act can help establish this trust between consumers and organisations. If an organisation clearly adheres to the act's principles, it shows the consumer that they value and protect their information, thus earning their trust. With swift developments in technology and the growing value of data, all parties involved (governments, individuals, and corporations) have a responsibility to create relationships wherein they defend privacy and trust (Richard & Hartzog, 2017). Digital marketing firms have a responsibility to ensure these relationships are created through data governance frameworks, while governments can ensure them through laws and regulations. Consumers have a responsibility to demand ethical collection, analysis, and use of their personal information.

Privacy as Power

Véliz, as cited by Wilsdon (2022), defines privacy as power. She states that a lack of privacy becomes a lack of power (over personal information) (Wilsdon, 2022). Acquiring personal information means acquiring power. Technology companies, therefore, hold a lot of power since they have thousands of people's personal information (Wilsdon, 2022). Consumers can exercise their power by taking control of their personal information and deciding who or what can have access to that personal information.

Privacy as Contextual Integrity

Nissenbaum (2004) defines privacy as contextual integrity – the author states that privacy, how it is viewed and accepted, changes with context. Contextual integrity is upheld if the gathering and distribution of information are appropriate for the specific context (Nissenbaum, 2004). If the gathering is not appropriate and the distribution is not within the norm, contextual integrity has been violated (Nissenbaum, 2004). This definition of privacy aligns with one of the PoPI Act's principles – purpose specification – which states that the entity possessing consumers' data is required to inform individuals why their information is being collected and how it will be processed (Breaker-Rolfe, 2023). Within the digital space, context can often become blurred, if a consumer agreed to a privacy policy – without truly comprehending the complicated terms in it, was the context for giving consent appropriate? Can privacy invasion – or at least violation be dismissed in this context? This study aims to determine consumers' answers and attitudes to those questions.

Brand Trust

Delgado-Ballester, Munuera-Alemán, and Yagüe-Guillén (2003) define brand trust as an assumption that a brand will act reliably and with positive intentions in a situation where there is some degree of risk to a consumer. Delgado-Ballester *et al.*, (2003) state that this assumption can be interpreted as a psychological state made up of certain trust expectations. The result of these expectations is that consumers believe trusting a brand will result in a positive outcome for them (Delgado-Ballester *et al.*, 2003).

This definition can be broken down into 2 key components namely, brand reliability and brand intentions (Delgado-Ballester *et al.*, 2003). Brand reliability refers to the perception that a brand will meet consumers' needs in a predictable and pre-agreed-upon manner (Delgado-Ballester *et al.*, 2003). If a brand is reliable, a foundation for trust can be built (Delgado-Ballester *et al.*, 2003).

The second component, brand intentions, refers to the belief held by consumers that a brand will act in a way that is favourable to their interests and will in no way take advantage of them or their information, no matter the situation (Delgado-Ballester *et al.*, 2003). Ultimately, this means the consumer is vulnerable, is aware of that, and trusts that brands will not take advantage of their vulnerability (Delgado-Ballester *et al.*, 2003).

This theory of brand trust puts most of the responsibility to uphold brand trust on the brand itself. Although this definition also leads to a very subjective understanding of brand trust

(Delgado-Ballester *et al.*, 2003) it is a fitting theory used as the understanding of privacy is also subjective and multi-faceted.

Literature Review

There is a need for more extensive academic and legal research to be done on the topic of digital privacy (Martin & Murphy, 2017). Existing literature will be analysed to gain an understanding of the key concepts of this study and how they impact consumer privacy. The four sections and their respective sub-sections are linked to the research questions and objectives of this study, the goal is that the review will indicate possible avenues for this research project to explore and help guide the research process.

Ways Consumer Privacy is Affected

Data is the single most valuable resource within the digital economy (Engels, 2019). Consumer data is used to personalise marketing communications and offerings, furthermore, data can be sold to third parties at a high price (Martin & Murphy, 2017). A wealth of data has led to considerable success in digital marketing activities – it could not be done without consumer information (Martin & Murphy, 2017). These facts incentivise marketers to gather as much personal information about consumers as possible – occasionally in unethical ways such as prohibiting a consumer from using certain platforms or services if they do not provide personal information. Although consent is given in these cases, one could argue that there was no real choice since the service or product the consumer desired would be unattainable if they did not provide information. This poses the question – is a consumer's privacy still violated even if consent was given, or does it become a matter of unfair business practices and ethics? In the data-gathering phase of this research project, an attempt to answer that question will be made.

Digital marketing encompassed a variety of activities - most of which require data gathering to be successful (Martin & Murphy, 2017) - for this literature review, only a few notable activities will be discussed:

Activity	Definition	Privacy Concerns
Online Behavioural Targeting	Use of tracking technology to gather information about consumers which is used	Behavioural tracking technology is not always detected by the consumer (Martin & Murphy, 2017).

	to create a detailed consumer profile (Martin & Murphy, 2017).	This can leave consumers with a sense of being under constant surveillance when faced with highly personalised messaging that they did not indicate they are interested in (See Figure 1).
Geofencing	Tracking consumers' location and data to send out marketing messages once they are near a company's location (Quach <i>et al.</i> , 2022).	Location tracking makes consumers uncomfortable (see figure 1) – location services might be enabled on a mobile device but that does not constitute permission given for multiple brands to send marketing communications or for that information to be shared with others.
Big Data	Advanced information capture and analysis which allows massive amounts of data to be analysed and gathered (Wieczorkowski & Polak, 2017).	The extent of information organisations can gather on consumers, and how it is used to profile them, using this technology is unknown to many consumers. This leads to a high privacy risk with regard to unauthorised access of consumer data (Quach <i>et al.</i> , 2022). It is another ethical concern – although a consumer might have provided

		consent to sharing personal information it was not necessarily to the extent to which big data makes it possible.
Personalisation	The use of consumer information to personalise marketing communications, product offerings and more (Engels, 2019).	A very detailed consumer profile is required to make personalisation effective. How this data is gathered could be the cause of this activity becoming an invasive one.

Table 1: Invasive Marketing Practices

Attitude of Consumers

Research conducted by Engels (2019) found that most internet users are unnerved and uncomfortable with their data being gathered, analysed, and stored. Privacy concerns also grow when the data provided by consumers is used for something other than was originally stated when the information is sensitive in nature, and when the consumer is not overly familiar with the organisation gathering the data (Quach *et al.*, 2022). These sentiments are corroborated by the information in Figure 1.

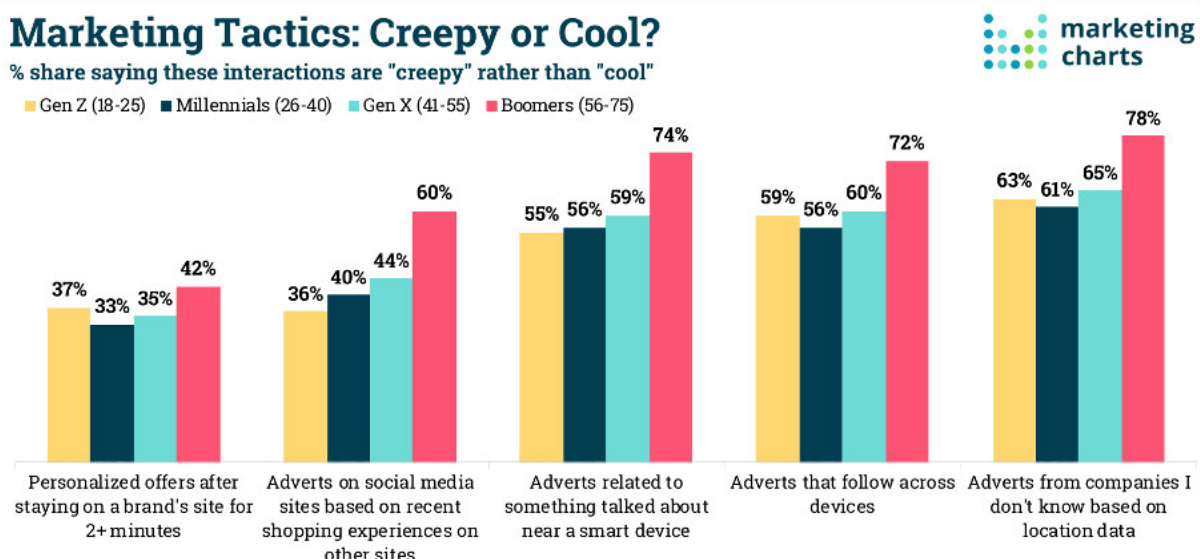


Figure 1: Marketing Charts; 2022 Marketing Tactics Creepy or Cool? (Marketing Charts, 2022).

The fifth graph in Figure 1 affirms what was discussed in the previous section about geo-fencing making consumers feel invaded. It also affirms that behavioural marketing is truly unsettling to some consumers.

Despite these concerns, Engels (2019) found that many consumers are willing to part with their data, even sensitive information if there is a benefit to them or a reward – such as exclusive deals. This indicates consumers can assign a value to their personal information, and as such to their privacy and violation thereof. If the pros outweigh the cons of privacy invasion, it is no longer of great concern for the consumer. Another indicator of this is that consumers are not willing to pay for an added level of privacy (Engels, 2019). The general attitude of consumers seems to be concerned with their information and how it is used by organisations, but they are not willing to forgo certain technologies or benefits to protect that information.

Consumer Control Over Personal Data

There is currently an unbalanced power structure when it comes to consumer data. Consumers have lost control of their data in the online context while organisations are now the power holders (Bandara, *et al.*, 2019). Advanced technologies not understood by the average consumer means they do not have the knowledge, power, or freedom to take back control of their data or confront the power imbalance (Bandara, *et al.*, 2019). This lack of knowledge makes it near impossible for consumers to make appropriate decisions regarding their data and it means they don't have total control over their personal information in the first place meaning they cannot be expected to carry the full responsibility of protecting it.

Considering the two dimensions of control over personal data, defined by Ashworth and Free (2006), discussed in the theoretical framework. It can be deduced that consumers are not aware of how their information is collected if they do not have the ability to make informed decisions or opinions on the matter. Additionally, the power imbalance means that the information used is in the hands of the organisation – creating a lack of awareness and control over the usage of personal information.

Consumers have attempted to take back control in multiple ways such as seeking social support and advice, doing background research on organisations, dissecting privacy policies, and using privacy-protecting technology (Bandara, *et al.*, 2019). These methods might have some success, but the fact that consumers were driven to act in such ways indicates the power imbalance regarding control over personal information and concern for digital privacy.

Consumers often sign over various rights to their information that they are not aware of. Privacy policies can be confusing for the average consumer – or in some cases even intentionally made to be incomprehensible (Martin & Murphy, 2017). In cases where a privacy policy was agreed to but not understood, no legal violation was committed, however, it is an ethical grey area. It can be argued that true consent is only given when all factors are completely understood – which is often not the case. This relates to the theory of brand trust. If a brand was fully trusted by consumers, meaning they acted reliably and with good intentions as discussed in the theoretical foundation, the issue could potentially have been avoided.

A final factor to consider regarding consumer control over privacy is the obstacles consumers must overcome to protect their information (Pike, 2020). If a consumer must take extensive action, possibly beyond their limited understanding, they will rather have their privacy violated (Pike, 2020). This also relates to the general consumer attitude discussed above, they care but also only to a certain extent. If it becomes an inconvenience to protect, they simply do not care enough to stop it. How much control does a consumer have over their personal information if they lack awareness and understanding? The discussion indicates little to none. The PoPI Act attempts to remove some of these obstacles consumers face (Accessible Law, 2019) specifically with two of its principles – processing limitation and openness. Processing limitation means consumer information is only collected and processed in a lawful and justified context while openness ensures that consumers are fully aware of what information an entity collects, how it is used, and who has access to it (Breaker-Rolfe, 2023).

Effect Of Invasive Marketing Practices

Effect on Consumers

The effect on consumers spans a variety of emotional and psychological factors. Firstly, consumers might feel threatened by data gathering, especially if they lack awareness of how it is gathered and then used afterwards (Bandara *et al.*, 2019). This feeling of threat could evolve into a feeling of complete distrust and resistance to sharing information, even when that information is gathered ethically and could be beneficial to the consumer. This is a defensive and reactionary stance that harms consumers' freedom to make decisions.

Another effect is the manipulation of consumers. If an organisation knows more about you than you are aware of, it can sway your opinions and manipulate your choice (Albulayhi &

Khediri, 2022). This was made evident in cases where social media marketers illegally helped political parties sway voter decisions by providing their data to political parties (Albulayhi & Khediri, 2022). This has a serious effect on consumers' freedom of choice, and many might not be aware of it.

Bandara *et al* (2019) found that repeated invasion of privacy can move beyond the feelings of threat or distrust to complete passiveness and powerlessness. Emotions such as these have a negative psychological effect. These effects on consumers relate to the theory of privacy of trust, consumers must be able to fully trust their information will not be used in any way that could lead to these negative outcomes.

One objective of this study is to determine the exact effects privacy invasion has had on individual consumers. Assumptions and connections can be made from previous literature but only the consumer affected can truly explain the short-term and long-term effects.

Effect on Brand Trust

Shih-Tse Wang (2018) found that brand trust – specifically relating to digital marketing activities – was formed around consumers' image of that brand online and how they conduct themselves. Because of this, it became evident that privacy concerns had a predominantly negative effect on brand trust. Additionally, Kelly *et al.*, (2017) found some consumers had more trust in technology companies – such as social media networks – with their data than they did in the brands who were actively targeting them with digital marketing using this technology.

Effect on Brands and Marketing Success

If consumers feel threatened and take the defensive stance mentioned above, a harmful market environment develops where the success of the market is affected (Bandara, *et al.*, 2019). After all, marketing is only successful if a consumer reacts (positively) towards it and supports the brand. Digital marketers and brands can strategically respond to this and promote the ethical and transparent collection and use of data (Bandara, *et al.*, 2019). The PoPI Act can make this strategic response easier for brands. By following the strict principles of the act, brands can rest assured knowing they are taking the necessary steps of handling data ethically and responsibly. This can create a competitive advantage for organisations. If a firm approaches data gathering in this way, they are more likely to be provided with rich and accurate data (Martin & Murphy, 2019). Consumers are also left with a positive brand

perception when they feel their privacy is being adequately protected (Martin & Murphy, 2017) this has many benefits for companies – from increased word of mouth to repeat sales.

How Brands Can Solve Privacy Problems

The power imbalance regarding control of personal information discussed earlier indicates that most of the responsibility – and true ability to have an impact - lies with organisations and marketers.

The first action organisations can take to prevent or solve privacy-related problems is simply to be responsible for their power and take extensive measures to protect consumers' privacy (Bandara *et al.*, 2019). Once information is in its possession, an organisation should follow their own (or a standard for its industry or country) data governance and protection systems. Organisations should also work to create the trust necessary for a positive experience regarding consumer privacy. Organisations should provide a detailed, and even more importantly understandable, privacy policy that even the most uninformed consumer can digest and understand (Bandara *et al.*, 2019). This relates to the concepts of data governance and trust – if governed correctly and ethically, consumers will happily trust organisations with their personal information. Adequate protection is also vital to preventing other privacy problems. Data breaches and scammers pose a massive threat to information consumers entrusted with organisations (Albulayhi & Khediri, 2022). If an organisation is a victim of such an attack and the loss of consumer information occurs, the negative effects for the company can be drastic. The relationship and trust are immediately broken.

Figure 2 below indicates ways in which organisations can build or win back consumer trust. It appears many consumers are willing to trust again if certain actions are taken. This indicates that if organisations conduct themselves ethically, follow a data governance framework, and promote trust, privacy-related problems should not be of much concern to them or consumers.

The Relationship Between Personal Data and Brand Trust

"Brands can improve my trust by:"

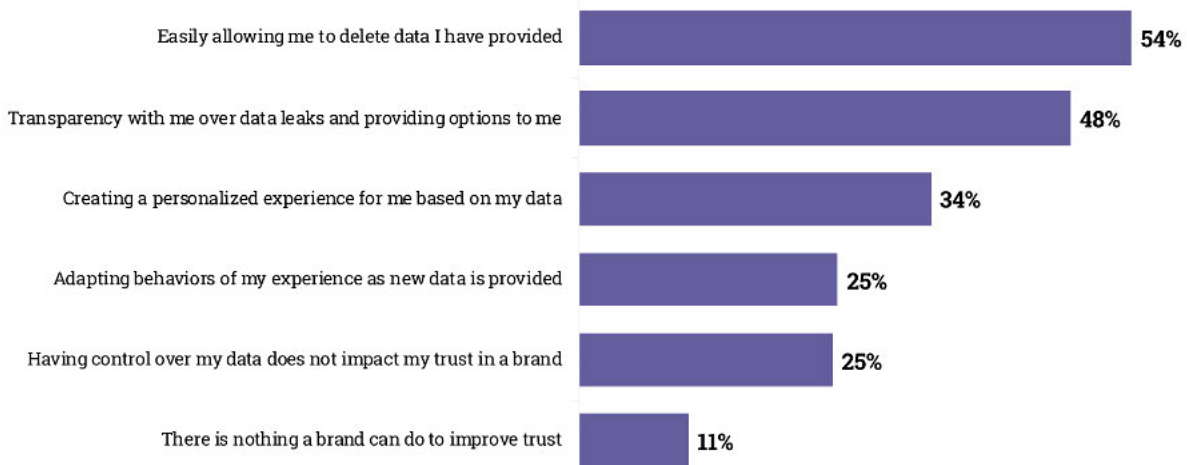


Figure 2: The Relationship Between Personal Data and Brand Trust
(Marketing Charts, 2022)

Conclusion

The general findings of this literature review indicate that there are multiple threats to consumer privacy. However, the attitudes of consumers vary from feeling threatened and angry to passive. Although there are privacy threats, there are many solutions as well, such as ethical data governance standards. Following the paradigm and related positions discussed at the beginning of the paper, this research project will continue to determine the effect privacy invasion has on individual consumers. The main concepts of this research were discussed in detail and interwoven with the literature review that followed. It revealed how interconnected all the themes of this study are with the key concepts. The appropriateness of the multi-definition approach to theorising privacy is clearer after the literature review section – it indicated that consumers' views about privacy all differ and their attitudes toward invasion thereof differ even more. Since this is the case, one definition would not have been appropriate. The brand trust definition is also proven to be appropriate, if a brand acts reliably and with good intentions, they are trustworthy and many, if not all, of the negative effects privacy invasion has on a brand and the trust consumers have in them, could be eradicated. Moving forward this study will aim to provide an even greater understanding of the themes in this paper.

Research Design & Methodology

Research Paradigm

A paradigm is defined by Kuhn (du Plooy-Cilliers, 2019) as a collection of beliefs which determines what researchers in various fields should study, how they conduct research, and how they interpret the results. A paradigm influences the way in which researchers study phenomena, and it determines the questions asked and procedures followed throughout the research process. The paradigm of this research project is interpretivism. Interpretive research incorporates human experience by acknowledging their beliefs, reasoning, and actions in social settings (Nickerson, 2022), the researchers learn about and acknowledge these by spending time with participants (du Plooy-Cilliers, 2019). Three aspects influencing the interpretive paradigm are worth mentioning:

1. Hermeneutics – how human actions are perceived and understood (du Plooy-Cilliers, 2019).
2. Phenomenology - how people perceive and understand their own experiences in the context of the norms of the world around them (du Plooy-Cilliers, 2019)
3. Symbolic interaction – a view accepting that the individual actions taken by humans have little meaning on their own, however, the actions of others are interpreted and understood and create a shared meaning, which in turn makes up the reality of humans (du Plooy-Cilliers, 2019).

This study aims to provide an understanding of how South African consumers are affected by data gathering for digital marketing practices and the implications thereof. Relating this to the phenomenological aspect of interpretivism, people's perception and understanding of data gathering and its effect on their digital privacy will be analysed. Participants' unique human experiences with data gathering and digital marketing will need to be studied to gain an understanding of the effect it has. To do this their own beliefs about what privacy is and digital marketing's effect on it will need to be determined, which will be possible by spending time with the participants and understanding their reasoning. For these reasons, interpretivism is the most appropriate paradigm to conduct this research as the findings will clarify the phenomena i.e., what privacy is within the digital age and how digital marketing activities affect it.

Ontological Position

Ontology relates to reality, what it is and what people know about it (see Research Design | Part 3 - Philosophy - Ontology, Epistemology, Axiology, Rhetoric, Methodology, 2020.). Within interpretivism, reality is seen as a social construct (du Plooy-Cilliers, 2019). It's subjective to individuals and their differing realities, all of which are valid and able to change as individuals' perceptions and experiences change (see Research Design | Part 3 - Philosophy - Ontology, Epistemology, Axiology, Rhetoric, Methodology, 2020). This relates to the symbolic interaction aspect of interpretivism – shared experiences create meaning and reality.

One person's idea of privacy is different to another's. This study aims to determine the participants' reality of digital privacy, how it is affected by digital marketing, how their trust in digital marketing and brands is consequently affected, and how this affects the success of digital marketing. Therefore, it looks at each participant's reality concerning data gathering and digital marketing. Considering the symbolic interaction aspect of interpretivism, one can say that the actions of digital marketers have an impact on the understood meaning participants hold about privacy and digital marketing's effect on it.

Epistemological Position

Epistemology refers to what knowledge is and how it's obtained – this then considers the relationship between a researcher and participant (see Research Design | Part 3 - Philosophy - Ontology, Epistemology, Axiology, Rhetoric, Methodology, 2020). Interpretive researchers look at facts within the context of people's interpretation of something – these facts can fluctuate depending on individual experiences and realities (du Plooy-Cilliers, 2019). This position is appropriate as the aim of this research project is to gather information (knowledge) about participants' unique experiences and perceptions of digital marketing's effect on privacy. This research is sensitive to context – when and how data is gathered, by whom etc. – and will not be generalised, which is another characteristic of an interpretivist epistemological position (du Plooy-Cilliers, 2019).

Axiological Position

Axiology refers to the values that make up a study and the researcher and how these affect the research process and findings (du Plooy-Cilliers, 2019). An interpretive position acknowledges and discusses all values that affect research, such as those of the researcher

and participants (du Plooy-Cilliers, 2019). For this study, the researcher and all participants have a subjective view of privacy – based on their values - and how it is affected by digital marketers' data-gathering techniques. Since research is bound by values in the axiological position of interpretivism it is understood that all research will be subjective to a degree (Dudovskiy, 2022). One of the questions this study aims to answer is what effect invasive data-gathering techniques have on South African consumers – this effect is completely subjective depending on the individual participant, and how serious this effect is for others, such as the researcher or readers of the study is also completely subjective.

Research Design and Approach

Research Design

This study followed a qualitative research design. There are a few differentiating features of qualitative research, one being that it typically relies on words and data based on meaning rather than numerical and statistical data (Maree, 2019). This study aimed to understand the first-hand experience of consumers and what it means for their trust in and relationships with brands, so a qualitative research design was most suitable. Maree (2019) states that qualitative research examines people in real-life social settings and how they navigate these settings. In this case, the social setting could be seen as consumers' interactions with brands. Bezuidenhout (2019) notes that qualitative research is subjective, from the researcher, instrument, and participant's perspective indicating that meaning is derived from the research results and interpreted differently according to the reader. This tied in with the interpretive paradigm underlying this study. Interpretivism studies and understands social settings and human behaviour and to do this, direct contact should be spent with the research participants (Bezuidenhout, 2019). Understanding how consumers behave after their experience with brands who have in some way invaded their privacy through digital marketing activities (the social setting) was what this study set out to do. Thus, making an interpretive paradigm and qualitative research design the most appropriate.

Type of Reasoning:

An inductive reasoning approach was utilised for this study. When a study recognises themes and patterns through analysis with no predetermined framework to directly guide these, it is inductive (Bezuidenhout, 2019). It is a reasoning approach that moves from the effect of a phenomenon to its cause, moving from general to specific (Bezuidenhout, 2019). In this case, the effect was that brand trust is diminished by the cause of digital marketing

activities. This is a bottom-up approach to research, it builds on a theory that is identified in research (Bezuidenhout, 2019).

Type of Research:

This was an exploratory study. When a research topic focuses on an unexplored or new area, it is an exploratory study (Swedberg, 2020). Understanding the effects of privacy invasion on brand trust remains an under-researched topic (this is explained further in the limitations of this study section). Davis (2019) list a few purposes on which exploratory research is based, the first is to determine the consequences of research problems. The research problem of this study was that digital marketing activities are an invasion of consumer privacy, and this has a consequent effect on consumers' trust in brands. The second purpose is to confirm assumptions (Davis, 2019). The assumption made was that digital marketing is an invasion of privacy. As discussed in the theoretical foundation section, privacy and the invasion thereof are highly subjective concepts, and not everyone will have the same definition of it. So, it was only an assumption that digital marketing invades the population of this study's privacy and that it negatively impacts brand trust. The final purpose of exploratory research, which is relevant, is that it aims to understand situations, conditions, or behaviours (Davis, 2019). This study aimed to understand how consumers are affected by privacy invasion (the situation) driven by digital marketing activities (the conditions) and how this affects their trust in the brands responsible for digital marketing activities (behaviour).

Time-Dimension:

Data was gathered for this study using a cross-sectional approach, meaning data was only gathered from the population at one specific point in time (Wang & Chen, 2020). The biggest motivator for this was the time constraints of this study.

Population

A study's population is defined by Davis (2019) as the people or things which hold the characteristics that relate to a researcher's interest and study. A study's population can be split into the target and accessible populations (Pascoe, 2019). All the people that fit the population parameters constitute the target population (Pascoe, 2019). Population parameters are the features shared by a population of a study (Pascoe, 2019). Pascoe

(2019) goes on to categorise population parameters into the nature, size, and characteristics of a population.

The population parameters of this study included:

Nature: People

Size: 5 participants

Characteristics: The people should have been affected by privacy invasion of invasive digital marketing practices in some way.

Thus, the target population of this study included consumers who have been affected by invasive digital marketing activities in some way.

The people that the researcher can access and include in a study are referred to as the accessible population (Pascoe, 2019). To narrow down the population into an accessible one, the population parameters were further narrowed down by location and age. The new parameters included:

1. Consumers living in Johannesburg or Cape Town.
2. Consumers between the ages of 30-50.

Thus, the accessible population of this study included South African consumers living in Johannesburg or Cape Town between the ages of 30-50 who have been affected by invasive digital marketing activities in some way.

The unit of analysis for this study was people.

Sampling

The population of this study was particularly specific and difficult to access. For this reason, two non-probability sampling methods were used. Non-probability sampling is effective when the population is difficult to narrow down or access (Pascoe, 2019). The first method used was snowball sampling using a screening questionnaire (See Annexure A for a copy). According to Pascoe (2019), this method makes use of referrals to access people who fit the population parameters. A screening questionnaire was sent out on social media by the researcher and others asked by the researcher. The asking of other people to send out the screening questionnaire is what made this part of the sampling the snowball method. Du Pascoe (2019) state that snowball sampling is an effective method to use when a population

is difficult to find. There are no databases or public records where individuals that fit this study's population parameters are listed and thus, snowball sampling using a screening questionnaire was the best method that led to finding reliable participants.

Due to the specific parameters of this study's population – particularly the characteristic that participants should have some experience with digital privacy invasion driven by digital marketing practices – only using snowball sampling would not have been suitable for accessing relevant participants, to solve this problem, purposive sampling was implemented on the screening questionnaire respondents. With a purposive sampling method, the characteristics of a population are purposely chosen (Pascoe, 2019). These characteristics are determined based on the research questions and population parameters (Pascoe, 2019). This ensures the entire sample consists of individuals who will sufficiently assist in answering the research questions (Pascoe, 2019). Based on the screening questionnaire responses, only the individuals who have experienced privacy invasion were chosen for the final data-gathering phase. Another motivator for implementing purposive sampling after snowball sampling is that this was a qualitative study with time constraints, meaning the sample size could not be large. Only a few highly relevant and suitable participants were required. To find these participants, purposive sampling was the most effective as the participants could be chosen with the final research questions and objectives in mind.

Due to time constraints and this being a qualitative study which required an in-depth analysis of respondents' interview questions, the sample size was capped at 5.

Data Collection

The data collection method was an in-depth interview. This method consists of conversations and helps a researcher learn more about participants' views, opinions, and beliefs on a particular topic (Strydom & Bezuidenhout, 2019). This is a qualitative data collection method used in qualitative studies (Strydom & Bezuidenhout, 2019) and assisted in understanding participants' experience with invasive digital marketing activities. The interview questions were created based on previous literature analysed throughout the duration of this study. With in-depth responses, all five research questions and objectives could sufficiently be addressed. The type of interview used was an open-ended interview. This is a more focused form of in-depth interviews that ask the same questions to all participants, making analysis easier and more organised (Strydom & Bezuidenhout, 2019). Due to time constraints, this assisted in analysing all the different experiences and opinions

in a more timely and organised manner. A copy of the instrument is attached in Annexure B.

The data collection method was implemented by meeting with each respondent individually via Microsoft Teams. The data was collected over a period of three days, from 27 July 2023 to 31 July 2023. It took an average of 25 minutes to conduct each interview. The meetings were recorded and automatically transcribed using Microsoft Teams' transcription tool. Before recording each respondent was informed of the fact that the interview would be recorded to align with ethical requirements. Once recording began, all interview questions were asked in the order.

Data Analysis

Data was analysed using a narrative analysis method. According to Maree (2019), this analysis method extracts meaning from narratives created during data collection. The method follows stories in data in order to unravel a common thread (Maree, 2019). Each participant had a different story about their experience with privacy invasion and how it has impacted their trust in brands. This method assisted in finding the necessary commonalities between these stories which effectively answered the research questions. Maree (2019) outlines 6 steps to narrative analysis:

1. Transcribe verbal material collected.
2. Organise text into indexical and non-indexical material. Indexical material refers to concrete references (Maree, 2019). Non-indexical material refers to values and judgements (Maree, 2019).
3. Analyse the events in an order according to the indexical material.
4. Analyse the non-indexical dimensions according to opinions, concepts, and theories.
5. Cluster and compare individual experiences.
6. Establish similarities and complete synthesis.

Narrative analysis deals with data at different levels to unravel all stories and find commonalities (Maree, 2019). Finding this common thread helped answer the general question of how invasive digital marketing affects brand trust. It also created a clear understanding of individual human experiences in this context.

The interview questions and their subsequent answers were broken up into indexical and non-indexical sections. The answers to each question were summarised (since all

respondents have had some experience with privacy invasion/invasive practices, there were many themes and similarities from the beginning, simplifying the summarisation process greatly) to create a general theme/answer to the question. This general theme was compared to the literature analyses and research done in previous assignments to determine how these respondents matched the theories and previous research or showed new trends. A more in-depth interpretation was then completed for each question by taking specific excerpts from individual interviews and using them to justify the themes further. By doing so step 6 of narrative analysis was complete, similarities were found and synthesis complete.

Findings & Interpretation of Findings

Indexical Material:

Indexical material refers to concrete references (Maree, 2019). The indexical material was identified using the following interview questions. In some cases, the interview questions were combined to group the indexical material better – e.g. question 3 and the material derived is a combination of questions 5 and 6 of the interview. These questions relate back to, and are in some cases very similar, to the original research questions and objectives. This is because all interview questions were written to address these and create a common thread throughout this study.

1. What do participants consider to be an invasion of privacy?

Participants in the study expressed various concerns about what they considered an invasion of their privacy. These concerns primarily revolved around:

Spam: Participants view spam phone calls, text messages, and emails to be highly invasive. They felt annoyed and intruded upon when their personal communication channels were bombarded with unsolicited messages.

Data Selling: Another significant concern was companies selling their personal information to third parties. This practice was seen as a breach of trust, as participants expected their data to be kept confidential. There was a specific emphasis on cell phone numbers being shared without consent, which often led to spam calls. This sharing of phone numbers was seen as a particularly intrusive invasion of privacy.

Targeted Advertising: Participants also felt uneasy about seeing advertisements for products or services they had searched for online without actively informing the company of their interest. This suggested to them that their online activities were being closely monitored without their explicit consent.

The targeted advertising aligns with previous literature. Behavioural tracking technology is not always detected by the consumer (Martin & Murphy, 2017). This can leave consumers with a sense of being under constant surveillance when faced with highly personalised messaging that they did not indicate they were interested in. However, all other invasive practices identified in the literature review – geofencing, big data, and personalisation – were

not mentioned by any respondents. This could be due to their own prioritisation of activities or knowledge of these activities.

2. How much control do participants believe they have over their data?

Participants had varying perceptions of how much control they had over their personal data:

Moderate Control: Some participants believed they had a moderate degree of control over their data. They likely referred to their ability to adjust privacy settings or manage their online presence to some extent.

“Somewhat, because I can choose what I search for, but I'm not stupid and I know the moment I search for something or click on something or look at something, there's an algorithm that's going to pick that up. I don't expect it not to happen.”

Lack of Education: Others expressed feeling uninformed or inadequately educated about how their information was handled. They didn't believe they had control because they lacked knowledge about the mechanisms involved.

“So, I feel that we probably have more control than we realise, but I also don't think that we are educated enough or that the information is readily available to understand how you can set your privacy settings in the way that would work for you.”

No Control: A few participants felt they had no control over their data, possibly due to a sense of resignation regarding data collection and usage by technology companies. They understood that algorithms were constantly tracking their online activities.

“No, I don't. I don't feel like I have any kind of control regardless of whatever privacy settings I use. I've accepted that we live in a world where everything is collected and it doesn't matter whether you are told that messaging, for example, is end to end encrypted, I'm well aware that there are companies that can track and trace all of those things. So even your WhatsApp conversations are not necessarily private, despite the fact that they say they are.”

“No, I know you know the moment I search for something or click on something or look at something that there's an algorithm that's going to pick that up. I don't expect it not to happen.”

Respondents' feelings of control correlate with previous literature and research done. Advanced technologies not understood by the average consumer means they do not have the knowledge, power, or freedom to take back control of their data or confront the power imbalance (Bandara, Fernando, & Akter, 2020).

3. Which activities do participants find to be invasive?

Participants identified specific activities they found invasive in the context of online interactions:

Excessive Information Sharing: Sharing too much personal information, especially phone numbers, when signing up on a website or making a purchase was deemed invasive. Participants were uncomfortable with the idea of sharing more than what they considered necessary.

“Phone number is probably the worst one.”

Information Selling: Nearly all respondents believed their information was being sold to third parties, leading to unsolicited calls and emails. This practice was seen as a significant betrayal of trust, indicating a link between informed consent and privacy invasion.

4. Has an experience ever negatively impacted consumers' trust in a brand?

Each participant has had their trust negatively impacted in some way through the sharing of their personal information. The participants all mentioned the brand name and type of brand. A theme emerged that participants were particularly trust-sensitive toward financial institutions and insurance companies – many respondents have experienced these organisations acting in an untrustworthy manner with their data.

“I mean goodness, Absa was subject to the most hacks and information and data leaks. I mean, I think they've worked very hard, I think, to regain the confidence of their own customers and clients because of that. So, it always nags you at the back

of your mind, but you know banking is something that's necessary. You have no choice.”

“I know that a specific bank has shown up on research as the worst performing bank in terms of digital safety and customer information safety. So that for me is a concern because it's [information leak] happened twice to me and the reason that I was given by my bank was, but you must have done a lot of like digital purchases somewhere, and I had not.”

This negative impact correlates with previous literature. Wang and Baker (2022) found that brand trust – specifically relating to digital marketing activities – was formed around consumers' image of that brand online and how they conduct themselves. Because of this, it became evident that privacy concerns had a predominantly negative effect on brand trust.

5. How can organisations minimise privacy concerns?

Participants offered insights into how organizations could address privacy concerns effectively:

Transparency: A recurring theme was the importance of transparency. Respondents emphasized that organizations should be open and honest about how they collect, use, and protect personal data. Transparent practices would build trust.

“Transparency. For example, it helps that with any Apple App you download, it asks you, would you like this to allow the app to track your online or not. Depending on the app, you allow the user to decide for himself.”

Ethics: Ethics played a crucial role in minimizing privacy concerns. Participants expected brands to follow ethical guidelines and treat their data with respect. Unethical practices such as data selling eroded trust.

“I think the human element needs to be tackled. People that work with information need to be more aware, or the training needs to be more rigorous in terms of how serious it is to have someone's information.”

Privacy Regulation: Many participants believed that existing privacy regulations were sufficient. They saw the responsibility for privacy protection shifting to the organizations themselves. Meeting or exceeding regulatory standards was seen as a minimum requirement.

“I would prefer if I'm dealing with you as a client one-on-one that my information only stays with you. I mean it is illegal actually for them to sell it already, but obviously that's happening anyway.”

Better Communication: Respondents advocated for improved communication from brands. Clear, concise, and easy-to-understand explanations of data handling practices and privacy policies would help alleviate concerns.

“More transparency, better communication.”

Non-Indexical Material:

Non-indexical material refers to values and judgements (Maree, 2019). Non-indexical material was identified in the same way as indexical material. By analysing different responses to interview questions and finding similarities/common threads.

1. How participants feel about invasive digital marketing practices.

Participants shared their emotional responses to invasive digital marketing practices, shedding light on their sentiments:

Anger: Some respondents expressed anger when confronted with invasive practices. They directed their frustration towards both the company that sold their information and the one that utilized it. This anger likely stemmed from a sense of violation and betrayal.

“I get angry at both the company that sold the information and the one that used it.”

Annoyance: Annoyance was a prevalent emotion among participants. They found invasive marketing practices to be bothersome and disruptive to their online experience. This annoyance was closely linked to the perceived invasion of their privacy.

“It annoys me to be quite honest because there is no privacy anymore.”

Frustration: Frustration was another common sentiment. Participants felt frustrated by the diminishing sense of privacy in the digital age. They yearned for a more private and controlled online environment.

Conditional Acceptance: Interestingly, some participants indicated that they didn't mind targeted advertising when it was relevant to their interests or for research purposes. This suggests that, under certain conditions, participants were open to engaging with digital marketing.

“I don't mind it when it's for products I like and, and if it's for companies I like. And I don't mind if it's for research.”

This information backs up research conducted by Engels (2019) that found most internet users are unnerved and uncomfortable with their data being gathered, analysed, and stored. However, if the pros outweigh the cons of privacy invasion, it is no longer of great concern for the consumer (Engels, 2019).

2. How have participants' relationships with and trust in brands been impacted by individual experiences?

Participants recounted how their personal experiences with brands had affected their relationships and trust:

Negative Impact on Relationships: All participants reported a negative impact on their relationships with brands that engaged in invasive practices. This impact ranged from completely discontinuing business with the brand to approaching it with caution and wariness. The experiences made participants more cautious about interacting with such brands in the future.

“The thing is basically when people do that, I will never ever click on that ad and I will never, ever use that product. I will block them.”

Trust Erosion: Trust in these brands was significantly eroded due to invasive marketing tactics. Participants mentioned that they were less likely to trust a brand that engaged in such practices.

“I’m always wary and scared when I do anything online.”

However, some brands with strong and credible identities were able to regain trust over time.

“One feels secure, one feels better with them. And I’m sure that that has to do with brand identity, confidence in the brand, which I think is linked to everything. The way that they market themselves as a brand in its entirety, the quality of their product, right down to the quality of their service.”

Brand Identity Matters: The credibility of a brand's identity played a crucial role in whether participants were willing to give a brand a second chance. Factors like the quality of the product and the overall brand image influenced participants' decisions to rebuild trust.

“And I’m sure that that has to do with brand identity, confidence in the brand, which I think is linked to everything, the way that they market themselves as a brand in its entirety, the quality of their product, right down to the quality of their service.”

3. How have participants’ experiences impacted their perception of digital marketing activities in general?

Participants' personal experiences had a notable impact on their perception of digital marketing activities:

Increasing Distrust: Participants shared that their experiences had made them more distrustful of digital marketing in general. They became more sceptical, especially when marketing efforts came from financial services institutions and banks.

“I do find myself becoming more and more distrusting of digital marketing and especially when it comes from sort of financial services institutions and banks.”

This increasing distrust reflects the broader trend of consumers becoming more cautious and critical of digital marketing practices, particularly in sensitive sectors like finance. If consumers feel threatened and take the defensive stance mentioned above, a harmful market environment develops where the success of the market is affected (Bandara, *et al.*,

2019). It suggests that brands need to be mindful of the long-term impact of invasive practices on consumer trust and perceptions of the industry as a whole.

Addressing The Research Question, Problem, and Objectives

Questions

Primary:

1. How does online data gathering, driven by digital marketing activities, impact on consumer relationships and brand trust?

Based on the findings, online data gathering driven by digital marketing activities has a significant impact on consumer relationships and brand trust. Participants reported a range of negative emotions, including anger, annoyance, and frustration when faced with invasive digital marketing practices. These invasive practices led to a deterioration of consumer relationships with brands, with some participants completely discontinuing their engagement with such brands. Trust in these brands was eroded, although some brands with strong and credible identities were able to regain trust over time. This suggests that online data gathering, when perceived as invasive, can harm consumer-brand relationships and trust.

Secondary:

2. When do consumers perceive data gathering to be an invasion of digital privacy?

Consumers perceive data gathering to be an invasion of digital privacy when it involves practices such as spamming (phone calls, text messages, and emails), the selling of personal information to third parties, and the display of targeted advertisements without active user consent. Specific emphasis is placed on the sharing of personal information, especially phone numbers, without consent, which often results in spam calls. This perceived invasion of privacy is linked to feelings of anger, annoyance, and frustration.

3. How is the success of digital marketing and online brands impacted by this experience with privacy invasion?

The success of digital marketing and online brands is negatively impacted by experiences with privacy invasion. Participants indicated that their relationships with brands were negatively affected, leading to a loss of business or increased wariness when interacting with these brands. Trust in the brands engaging in invasive marketing practices was eroded, and this erosion of trust had a lasting impact. However, brands with credible identities had a better chance of regaining trust over time. Overall, privacy invasion experiences can damage a brand's reputation and success in the digital market.

4. How is the control of consumers over their information affected by digital marketing activities?

Participants had varying perceptions of control over their data. While some believed they had moderate control, others felt uninformed and lacked control due to their limited understanding of data handling. A few participants felt they had no control, likely due to a sense of resignation regarding data collection by technology companies. This suggests that digital marketing activities can affect consumers' perceived control over their information, influencing their level of comfort and trust in online interactions.

5. How does the experience of consumers affect their trust in and relationships with brands?

The experiences of consumers, particularly in encountering privacy invasion, have a direct impact on their trust in and relationships with brands. Participants reported negative emotions and behaviours, such as anger, annoyance, discontinuation of engagement, and wariness when dealing with brands that engaged in invasive practices. Trust in these brands was eroded, although some could regain it over time. This indicates that consumer experiences significantly affect their trust in and relationships with brands, emphasizing the importance of ethical and transparent digital marketing practices for maintaining positive consumer-brand interactions.

Problem

The problem is that consumers are being affected by unethical digital marketing activities and that possibly hurts brand trust.

The data gathered highlights several key aspects of this problem:

Impact on Consumers: Consumers experience negative emotions, including anger, annoyance, and frustration when exposed to invasive digital marketing practices. These practices involve activities such as spamming, selling personal information, and displaying targeted ads without explicit consent. This suggests that consumers perceive these activities as unethical and invasive.

Erosion of Trust: The experiences of consumers with these unethical marketing practices are negatively impacting their trust in brands. Trust is a critical component of consumer-brand relationships, and when trust is eroded, it can lead to consumers being wary of engaging with these brands or even discontinuing their business relationships altogether.

Brand Reputation: Brands engaging in unethical digital marketing practices risk damaging their reputation. Participants in the study reported that their relationships with brands were negatively affected, and this could potentially result in long-term harm to a brand's success in the digital market.

Consumer Control: Consumers' perceived control over their personal information is also influenced by digital marketing activities. Some consumers feel they have limited control due to their lack of understanding of data handling practices, while others perceive themselves as having no control. This suggests that unethical marketing activities can contribute to a sense of powerlessness among consumers regarding their data.

In summary, the research problem centres on the ethical implications of digital marketing activities and their consequences for both consumers and brands. Unethical practices not only evoke negative emotions in consumers but also erode trust in brands, potentially harming brand reputation and success. Addressing this problem involves understanding the factors that contribute to consumer dissatisfaction and finding ways to promote ethical and transparent digital marketing practices to mitigate these negative effects on both consumers and brands.

Objectives

1. Determine which digital marketing activities affect consumer privacy.

The research provides insights into the specific digital marketing activities that impact consumer privacy. Participants highlighted activities such as spamming through phone calls, text messages, and emails, the selling of personal information to third parties, and the display of targeted advertisements without active user consent as practices that they considered invasive. This information identifies the digital marketing activities that affect consumer privacy.

2. Understand the attitude of consumers towards these digital marketing activities.

The research sheds light on consumers' attitudes towards invasive digital marketing activities. Participants expressed their feelings of anger, annoyance, and frustration when faced with these practices. Some also mentioned conditional acceptance, indicating that they might tolerate such activities if they are relevant or for research purposes. Understanding these attitudes helps uncover the emotional and behavioural responses of consumers to these activities.

3. Determine how much control consumers had or have over their data.

Participants' perceptions of control over their data were discussed in the research. Some believed they had a moderate degree of control, while others felt uninformed and lacked control due to their limited understanding of data handling. This information helps determine the varying levels of control that consumers perceive they have over their data in the context of digital marketing activities.

4. Determine how organisations can help minimise or solve privacy concerns.

The research provides insights into how organizations can address privacy concerns effectively. Participants emphasized the importance of transparency and ethics. They believed that privacy regulations were sufficient and that it was up to brands to communicate openly and honestly about their data handling practices. This information offers guidance on potential solutions, emphasizing the need for transparent communication and ethical behaviour by organizations.

5. Understand how invasive data gathering affects South African consumers' trust in and relationship with brands.

The research directly addresses this objective by showcasing how invasive data gathering impacts South African consumers' trust in and relationships with brands. Participants reported a negative impact on their relationships with brands that engaged in invasive practices. Trust in these brands was eroded, leading to behaviours such as discontinuing engagement or approaching these brands with caution. Some brands were able to regain trust over time, highlighting the complex dynamics between privacy invasion and consumer-brand relationships in the South African context.

Conclusion

Trustworthiness

Assessing the trustworthiness of data is a crucial step in qualitative data (Maree, 2019).

There are 4 categories of trustworthiness for qualitative research:

1. **Credibility**

Credibility refers to the reality and believability of findings (Maree, 2019). It's ensured by utilising well-established research methodology and design that relate to the research question and theoretical framework (Maree, 2019). The methodology of this study fits well with the theoretical framework and paradigm discussed in the sections above. The sampling, data collection, and analysis methods are all qualitative methods and will effectively assist in answering the research questions.

2. **Transferability**

Transferability means readers can connect components of the study (Maree, 2019). It is ensured by using contextually relevant participants and applying the findings accurately within the given context (Maree, 2019). As discussed in the sampling section, the participants will be highly relevant and source with purpose and great consideration. Additionally, the narrative analysis method will assist in creating links between the data to relate the findings to the research questions and objectives.

3. **Dependability**

Dependability is ensured by implementing the research design and methodology effectively (Maree, 2019). This will be done for this study by motivating all decisions taken throughout the research process, even if some of the methods change as the study progresses.

4. **Confirmability**

Confirmability means researcher and participant bias is kept to a minimum – as much as is possible (Maree, 2019). As discussed in the paradigm section, specifically the axiological position of interpretivism, all research is subjective to some degree. This will be minimised through a logical narrative analysis that removes opinions and rather focuses on the patterns and links between participants' experiences and thoughts on the research topic.

Anticipated Contribution

The first contribution of this research is the addition of information to the brand trust and digital privacy body of knowledge. The information can be used by South African brands to

understand how data gathering can affect the trust their customers have in them. The findings can be quantified and used to create a more generalized understanding of the topic. Which in turn, can be more widely used by brands. Lastly, the information can be used by South African consumers to learn about other South African consumers' experiences with digital privacy.

Ethical Consideration

There are several ethical considerations with research. For this study, the first consideration is bias in asking and answering questions. The participants will not be pushed to elaborate on answers to avoid an influence on their responses driven by researcher bias. All participants must be over 18 and give their full consent. Full transparency between the researcher and participants should exist. This is ensured by providing all participants with a consent form that they sign, a copy of which can be seen in Annexure A.

Limitations

The multifaceted nature of privacy makes it difficult to define. Participants might have varying ideas of privacy.

As a qualitative study, the findings cannot be generalised thus limiting the use of the findings. A lack of research done on the concept of digital privacy in the South African context makes literature difficult to find and assess.

Reference List

Accessible Law. 2019. Section 2 Purpose of Act, 11 July 2019. [Online]. Available at: <https://popia.co.za/section-2-purpose-of-act/> [Accessed on 17 November 2023].

Albulayhi, M. and Khediri, S. 2022. A Comprehensive Study on Privacy and Security on social media. *Journal of Interactive Mobile Technologies*, 16(1): 4-21. [Online]. Available at: <https://web-s-ebSCOhost-com.ezproxy.iielearn.ac.za/ehost/detail/detail?vid=10&sid=e1d75e66-2e6d-43df-a7da-8b2987c81dc7%40redis&bdata=JnNpdGU9ZWZWhvc3QtbGl2ZSZzY29wZT1zaXRl#AN=154752069&db=egs> [Accessed on 25 October 2022].

Ashworth, L. and Free, C. 2006. Marketing Dataveillance and Digital Privacy: Using Theories of Justice to Understand Consumers' Online Privacy Concerns. *Journal of Business Ethics*, 67: 107-123. [Online]. Available at: <https://web-s-ebSCOhost-com.ezproxy.iielearn.ac.za/ehost/detail/detail?vid=13&sid=f847757a-3853-474b-9fe7-766b94f76fd2%40redis&bdata=JnNpdGU9ZWZWhvc3QtbGl2ZSZzY29wZT1zaXRl#AN=22327814&db=bsu> [Accessed on 24 October 2022].

Bandara, R., Fernando, M. and Akter, S. 2019. Addressing privacy predicaments in the digital marketplace: A power-relations perspective. *Journal of Consumer Studies*, 44: 423-434. [Online]. Available at: <https://web-s-ebSCOhost-com.ezproxy.iielearn.ac.za/ehost/detail/detail?vid=3&sid=e1d75e66-2e6d-43df-a7da-8b2987c81dc7%40redis&bdata=JnNpdGU9ZWZWhvc3QtbGl2ZSZzY29wZT1zaXRl#db=agr&AN=IND607058371> [Accessed on 24 April 2022].

Breaker-Rolfe, J. 2023. Summary of South Africa's Protection of Personal Information Act (PoPIA), 4 September 2023. [Online]. Available at: [https://www.tripwire.com/state-of-security/summary-south-africas-protection-personal-information-act-popia#:~:text=South%20Africa's%20Protection%20of%20Personal%20Information%20Act%20\(PoPIA\)%2C%20also,took%20effect%20in%20July%202020](https://www.tripwire.com/state-of-security/summary-south-africas-protection-personal-information-act-popia#:~:text=South%20Africa's%20Protection%20of%20Personal%20Information%20Act%20(PoPIA)%2C%20also,took%20effect%20in%20July%202020). [Accessed on 17 November 2023].

Delgado-Ballester, E., Munuera-Alemán, J. and Yagüe-Guillén, M. 2003. Development and validation of a brand trust scale. *Journal of Market Research*, 45(1): 35-53. [Online]. Available at: <https://web-p-ebSCOhost-com.ezproxy.iielearn.ac.za/ehost/detail/detail?vid=6&sid=baa493fd-fa4d-42f0-9d63->

[92342a901f49%40redis&bdata=JnNpdGU9ZWhvc3QtbGl2ZSZzY29wZT1zaXRI#AN=9022195&db=bsu](https://www.sciencedirect.com/science/article/pii/S0950268820300000) [Accessed on 22 March 2023].

Du Plooy-Cilliers, F. 2019. Research Paradigms and Traditions. In: du Plooy-Cilliers, F., Davis, C. and Bezuidenhout, R. eds. 2019. *Research Matters*. Cape Town: Juta & Company Ltd, Chapter 2: 27-31.

Du Plooy-Cilliers, F. 2019. Research Paradigms and Traditions. In: du Plooy-Cilliers, F., Davis, C. and Bezuidenhout, R. eds. 2019. *Research Matters*. Cape Town: Juta & Company Ltd, Chapter 2: 27-31.

Bezuidenhout, R. 2019. Theory in Research. In: du Plooy-Cilliers, F., Davis, C. and Bezuidenhout, R. eds. 2019. *Research Matters*. Cape Town: Juta & Company Ltd, Chapter 3: 49.

Bezuidenhout, R. and Davis, C. 2019. From Topic to Research Question. In: du Plooy-Cilliers, F., Davis, C. and Bezuidenhout, R. eds. 2019. *Research Matters*. Cape Town: Juta & Company Ltd, Chapter 4: 69-70.

Davis, C. 2019. The Aims of Research. In: du Plooy-Cilliers, F., Davis, C. and Bezuidenhout, R. eds. 2019. *Research Matters*. Cape Town: Juta & Company Ltd, Chapter 5: 75-78.

Davis, C. 2019. The Research Rationale. In: du Plooy-Cilliers, F., Davis, C. and Bezuidenhout, R. eds. 2019. *Research Matters*. Cape Town: Juta & Company Ltd, Chapter 7: 97-98.

Pascoe, G. 2019. Sampling. In: du Plooy-Cilliers, F., Davis, C. and Bezuidenhout, R. eds. 2019. *Research Matters*. Cape Town: Juta & Company Ltd, Chapter 11: 132-144.

Strydom, A. and Bezuidenhout, R. 2019. Qualitative Data Collection. In: du Plooy-Cilliers, F., Davis, C. and Bezuidenhout, R. eds. 2019. *Research Matters*. Cape Town: Juta & Company Ltd, Chapter 13: 188-191.

Bezuidenhout, R. and Cronje, F. 2019. Qualitative Data Analysis. In: du Plooy-Cilliers, F., Davis, C. and Bezuidenhout, R. eds. 2019. *Research Matters*. Cape Town: Juta & Company Ltd, Chapter 16: 229-249.

Dudovskiy, J. 2022. Axiology, 2022. *Research Methodology*, date of publication. [Online]. Available at: <https://research-methodology.net/research-philosophy/axiology-2/> [Accessed on 27 October 2022].

Engels, B. 2019. Digital first, privacy second? Digital natives and privacy concerns. *International Conference e-Society*. [Online]. Available at: <https://web-s-ebsohost-com.ezproxy.iielearn.ac.za/ehost/pdfviewer/pdfviewer?vid=5&sid=f847757a-3853-474b-9fe7-766b94f76fd2%40redis> [Accessed on 24 April 2023].

Kelly, L., Kerr, G. And Drennan, J. 2017. Privacy concerns on social networking sites: A longitudinal study. *Journal Of Marketing Management*, 33(17/18),:1465-1489. [Online]. Available At: <https://web-p-ebsohost-com.ezproxy.iielearn.ac.za/ehost/Detail/Detail?Vid=4&Sid=Baa493fd-Fa4d-42f0-9d63-92342a901f49%40redis&Bdata=Jnnpdgu9zwhvc3qtbgl2zszy29wzt1zaxrl#An=127028823&Db=Bsu> [Accessed On 18 March 2023].

Mandal, P. 2019. Public Policy Issues in Direct and Digital Marketing – Concerns and Initiatives: Public Policy in Direct and Digital Marketing. *Journal of Public Administration in the Digital Age*, 6(4): 54-71. [Online]. Available at: <https://www.igi-global.com/pdf.aspx?tid=241267&ptid=200881&ctid=4&oa=true&isxn=9781522568438> [Accessed on 25 April 2023].

Maree, K. 2019. *First Steps in Research*. Pretoria: Van Schaik.

Marketing Charts, 2022. Marketing Tactics: Creepy or Cool? *Marketing Charts*, September 9 2022. [Online]. Available at: <https://www.marketingcharts.com/customer-centric/privacy-and-security-226847> [Accessed on 24 October 2022].

Marketing Charts. 2022. The Relationship Between Personal Data and Brand Trust. *Marketing Charts*, August 9 2022. [Online]. Available at: <https://www.marketingcharts.com/cross-media-and-traditional-226542> [Accessed on 25 October 2022].

Martin, K. and Murphy, P. 2016. The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, 45(2): 135-155. [Online]. Available at: <https://web-s-ebscohost-com.ezproxy.iielearn.ac.za/ehost/detail/detail?vid=7&sid=f847757a-3853-474b-9fe7-766b94f76fd2%40redis&bdata=JnNpdGU9ZWWhvc3QtbGl2ZSZzY29wZT1zaXRI#AN=121264032&db=bsu> [Accessed on 22 October 2022].

Nickerson, C. 2022. Interpretivism Paradigm & Research Philosophy. *Simply Sociology*, 5 April 2022. [Online]. Available at: <https://simplysociology.com/interpretivism-paradigm.html#assumptions> [Accessed on 18 October 2022].

Nissenbaum, H. 2004. Privacy as Contextual Integrity. *Journal of Law*, 79(1): 137-138. [Online]. Available at: <https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10/> [Accessed on 23 October 2022].

Pike, E. 2020. Defending data: toward ethical protections and comprehensive data governance. *Journal of Law*, 69: 687-742. [Online]. Available at: <https://web-s-ebscohost-com.ezproxy.iielearn.ac.za/ehost/detail/detail?vid=8&sid=e1d75e66-2e6d-43df-a7da-8b2987c81dc7%40redis&bdata=JnNpdGU9ZWWhvc3QtbGl2ZSZzY29wZT1zaXRI#AN=143867557&db=asn> [Accessed on 24 October 2022].

Research Design | Part 3 - Philosophy - Ontology, Epistemology, Axiology, Rhetoric, Methodology. 2020. YouTube video added by DRJ Thesising 101.[Online]. Available at: <https://www.youtube.com/watch?v=YV2JOJtP7E0> [Accessed on 20 October 2022].

Richards, N. and Hartzog, W. 2017. Privacy's Trust Gap. *Journal of Law*, 126(1180): 1213-1215. [Online]. Available at: <https://deliverypdf.ssrn.com/delivery.php?ID=538097071083087011079096104065118005042087014021019030101082088111071106065105115064101057053127049096017010087068117072092069116091005007014026100104073025101107123090065022008007104112066120092115101114002092091124025090089102085101085096121022121064&EXT=pdf&INDEX=TRUE> [Accessed on 22 October 2022].

Rollenhagen, L. 2020. Alan Westin is the Father of Modern Data Privacy Law, 8 September 2020. [Online]. Available at: <https://www.osano.com/articles/alan-westin#:~:text=In%20%E2%80%9CPrivacy%20and%20Freedom%2C%E2%80%9D,was%20revolutionary%20in%20its%20approach>. [Accessed on 20 October 2022].

Selinger, E. and Hartzog, W. 2014. Obscurity and Privacy. *Article*. [Online]. Available at: <https://deliverypdf.ssrn.com/delivery.php?ID=597095116095088018067024079101072002127063056052064082108094013005092111122114030075053003005120047011112020106071113014120125109082054028068110069078067065081125028041055009099127076120127065004099008012120077008010085094003103110102086093126113085092&EXT=pdf&INDEX=TRUE> [Accessed on 23 October 2022].

Swedberg, R. 2020. Exploratory Research. [eBook]. Available at: https://books.google.co.za/books?hl=en&lr=&id=vITMDwAAQBAJ&oi=fnd&pg=PA17&dq=exploratory+research&ots=ITuCiZPfWt&sig=PQelbdJsMROnHnRHro0L0U_S1qE#v=onepage&q=exploratory%20research&f=false [Accessed on 5 May 2023].

Turrecha, L. and Ashley, E. The rise of privacy tech: Defining the privacy Tech landscape 2021: A foundational whitepaper to help fuel privacy innovation. *Rise of Privacy Tech*, November 2021. [Online]. Available at: <https://www.riseofprivacytech.com/wp-content/uploads/2021/11/TROPT-Defining-the-Privacy-Tech-Landscape-2021-v1.0-1.pdf> [Accessed on 24 April 2023].

Wahyuningtyas, S. 2017. Abuse of Dominance in Non-Negotiable Privacy Policy in the Digital Market. *Article*, 18(4): 785-800. [Online]. Available at: <https://web-s-ebsohost-com.ezproxy.iielearn.ac.za/ehost/detail/detail?vid=6&sid=e1d75e66-2e6d-43df-a7da-8b2987c81dc7%40redis&bdata=JnNpdGU9ZWwhvc3QtbGl2ZSZzY29wZT1zaXRl#AN=126405820&db=asn> [Accessed on 25 October 2022].

Waldman, A. 2015. Privacy as Trust: Sharing Personal Information in a Networked World. *Journal of Law*, 69(3): 590-591. [Online]. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2309632 [Accessed on 22 October 2022].

Wang, X. And Baker, D. 2022. Criminalising Privacy In The Digital Age: The Reasonable Expectation Of Not Being Digitally Monitored. *Journal Of Criminal Law*, 86(3), 146-168. [Online]. Available At: <https://Web-P-Ebscohost-Com.Ezproxy.iielearn.Ac.Za/Ehost/Detail/Detail?Vid=2&Sid=Baa493fd-Fa4d-42f0-9d63-92342a901f49%40redis&Bdata=Jnnpdgu9zwhvc3qtbgl2zszy29wzt1zaxrl#An=157566574&Db=Asn> [Accessed On 17 March 2023].

Wang, X. and Chen, Z. 2020. Cross-sectional studies: Strengths, weaknesses, and recommendations. *Chest Journal*, 158(1): 65-71. [Online]. Available at: [sciencedirect.com/science/article/pii/S0012369220304621](https://www.sciencedirect.com/science/article/pii/S0012369220304621) [Accessed on 5 May 2023].

Wieczorkowski, J. and Polak, P. 2017. Big data and privacy: The study of privacy invasion acceptance in the world of big data. *Journal of Applied Knowledge Management*, 5(1): 57-71. [Online]. Available at: <https://web-p-ebscohost-com.ezproxy.iielearn.ac.za/ehost/detail/detail?vid=2&sid=921b284a-b1ce-4aef-a063-d58e658909c5%40redis&bdata=JnNpdGU9ZWwhvc3QtbGl2ZSZzY29wZT1zaXRl#AN=123292835&db=asn> [Accessed on 23 October 2022].

Wilsdon, L. 2022. Carissa Véliz, Privacy Is Power: Why and How You Should Take Back Control of Your Data. *Journal of Law*, 12(3): 255-257. [Online]. Available at: <https://academic.oup.com/idpl/article/12/3/255/6545822> [Accessed on 22 October 2022].

Yuvaraj, S. and Indumathi, R. 2018. Influence on digital marketing on brand building. *International Journal of Mechanical Engineering and Technology*, 9(7): 235-243. [Online]. Available at: https://d1wqtxts1xzle7.cloudfront.net/57190960/IJMET_09_07_027-libre.pdf?1534319851=&response-content-disposition=inline%3B+filename%3DINFLUENCE_OF_DIGITAL_MARKETING_ON_BRAND.pdf&Expires=1682595056&Signature=DvkZHjOteTdzYr4dvSxuPr-2yTGOF~5aXgc28v6A4pQJkYyduHnshRbn0HGDO~7eEBMEffTBQ9cn9fnyFSC8xuPJZdAG5np0qtklfa4ynkbjch7M8mG7NuZVByMUBwgEhPpo0QR6Az8u8LszAlhTU4LNT0Ve1Z2bGGIYTvmYPSK8fh0o43wy0~V1KTWdhkCKMfgV10wESXc3ojVEbQaKB0IRO5uqB62jHs2vwWPctjs4uzEFWUqPYsz9CKoXstO9Pm0GRyd1AHqHXWBH2P0APKFf43Ot1IDUjgat~9hZZ3uZKnnGOEKOngFsFOUM9CCobthpzUXZp64ppPq2J0zMUQ_&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA [Accessed on 24 April 2023].

Zeccherini, T. 2015. Privacy: theoretical analysis of the value of this concept for greater protection of personal data. *Thesis*. [Online]. Available at:

<https://deliverypdf.ssrn.com/delivery.php?ID=318115065115116113002067078003019087017069064045069066075089118069073000022122126018022103030104056120001029127085084008118093117022094008013007027024100118126001112065073085000066011018001112008088087085104066100090012111112107122027011119016090066074&EXT=pdf&INDEX=TRUE> [Access on 24 October 2022].

Annexure A: Example of Consent Forms

Participant Consent Form

Explanatory information sheet and consent form for participants
To whom it may concern, My name is Elke Stegmann and I am a student at The IIE's [REDACTED]. I am currently conducting research under the supervision of Mr Tiaan Ras about how privacy invasion driven by digital marketing activities affects consumers, their relationship with, and trust in brands. I hope that this research will enhance our understanding of digital privacy invasion's effect on consumers in the South African context and the importance of brand trust. I would like to invite you to participate in my study. In order to explain to you what your participation in my study will involve, I have formulated questions that I will try to fully answer so that you can make an informed decision about whether or not to participate. If you have any additional questions that you feel are not addressed or explained in this information sheet, please do not hesitate to ask me for more information. Once you have read and understood all the information contained in this sheet and are willing to participate, please complete and sign the consent form below.
What will I be doing if I participate in your study?
I would like to invite you to participate in this research because you are a suitable candidate to participate and assist me in answering my research question. If you decide to participate in this research, I would like to interview you to learn about your experience with digital privacy invasion and how this subsequently affected your perception of and trust in brands. The interview will be recorded for analysis purposes. You can decide whether or not to participate in this research. If you decide to participate, you can choose to withdraw at any time or to decide not to answer particular interview questions.
Are there any risks/ or discomforts involved in participating in this study?
Whether or not you decide to participate in this research, there will be no negative impact on you. There are no direct risks or benefits to you if you participate in this study. You might, however, indirectly find that it is helpful to talk about your experience with digital privacy invasion. If you find at any stage that you are not comfortable with the line of questioning, you may withdraw or refrain from participating.
Do I have to participate in the study?
• Your inclusion in this study is completely voluntary; • If you do not wish to participate in this study, you have every right not to do so; • Even if you agree to participate in this study, you may withdraw at any time without having to provide an explanation for your decision.
Will my identity be protected?

I promise to protect your identity. I will not use your name in any research summaries to come out of this research and I will also make sure that any other details are disguised so that nobody will be able to identify you. I would like to ask your permission to record the interviews, but only my supervisor, I and possibly a professional transcriber (who will sign a confidentiality agreement) will have access to these recordings. Nobody else, including anybody at Vega School, will have access to your interview information. I would like to use quotes when I discuss the findings of the research, but I will not use any recognisable information in these quotes that can be linked to you.

What will happen to the information that participants provide?

Once I have finished all interviews, I will write summaries to be included in my research report, which is a requirement to complete my BCom Honours in Strategic Brand Management. You may ask me to send you a summary of the research if you are interested in the final outcome of the study.

What happens if I have more questions about the study?

Please feel free to contact me or my supervisor should you have any questions or concerns about this research, or if there is anything you need to know before you decide whether or not to participate.

You should not agree to participate unless you are completely comfortable with the procedures followed.

My contact details are as follows:

Elke Stegmann

[REDACTED]

[REDACTED]

The contact details of my supervisor are as follows:

Mr Tiaan Ras

[REDACTED]

[REDACTED]

Participant or respondent consent

I, _____, agree to participate in the research conducted by Elke Stegmann about the effect of privacy invasion driven by digital marketing activities on consumers, their relationship with, and trust in brands This research has been explained to me and I understand what participation in this research will involve. I understand that: • I agree to be interviewed for this research. • My confidentiality will be ensured. My name and personal details will be kept private. • My participation in this research is voluntary and I have the right to withdraw from the research at any time. There will be no repercussions should I choose to withdraw from the research. • I may choose not to answer any of the questions that are asked during the research interview. • I may be quoted directly when the research is published, but my identity will be protected.	
Signature	Date

Audio or Video Recording Consent Form

Consent form for participants	
I, _____, agree to allow Elke Stegmann to audio record my interviews as part of the research about how privacy invasion affects consumers, their relationship with, and trust in brands. This research has been explained to me and I understand what participation in this research will involve. I understand that: • My confidentiality will be ensured. My name, personal details or any other identifiable information will be kept confidential; • The recordings will be stored in a password-protected file on the researcher's computer; and • Only the researcher, the researcher's supervisor(s) and possibly a transcriber (who will sign a confidentiality agreement) will have access to these recordings.	
Signature	Date

Quantitative Disclaimer

Although this was a qualitative study, a quantitative screening questionnaire was sent out during the sampling process. Making a quantitative disclaimer a necessary ethical clearance requirement.

Privacy In the Digital Age: Understanding the Effects of Privacy Invasion on Brand Trust

Informed Consent

The following survey is being conducted in line with the academic requirements of THE IIE VEGA SCHOOL Online. as part of the BCom Strategic Brand Management. My name is Elke Stegmann and the aim of my research is to enhance the understanding of digital privacy invasion's effect on consumers in the South African context and the importance of brand trust. Your participation in this survey is voluntary and open to participants who are over the age of 18 years old, living in Johannesburg or Cape Town, and has been affected in some way by privacy invasion. You may withdraw your participation at any time and there will be no penalties for withdrawal or non-completion of the survey. The procedure involves completing an online survey, which will take approximately 10 minutes to complete.

No personal information is required from you for the completion of this survey and all information will be kept anonymous. The findings of this research will be presented in the final Research Project submission to Vega, however, all collected data will be stored under a password-protected file on the researcher's computer for a period of five years.

The analysed results of this data will be shared for scholarly purposes only and shared with the academic coordinators of THE IIE VEGA SCHOOL Online RESE8419/w/p Module. This research has been reviewed and approved by The Independent Institute Of Education's ethical procedures regarding research involving human participants and Ethical Clearance has been granted. Should you have any concerns or questions, please do not hesitate to contact me on [REDACTED]

ELECTRONIC CONSENT: Please select your choice below.

Clicking on the "**agree**" button below indicates that:

- you have read and understood the purpose of this research study
- you voluntarily agree to participate in this research study
- you are over the age of 18 years

If you **do not wish** to participate in this research, please **decline** participation by clicking the "disagree" button.

☐ Agree

☐ Disagree

Annexure B: Measurement Instruments

Screening Questionnaire

1. How old are you?
 - 19 or younger
 - 20-30
 - 31 or older
2. Where do you live?
 - Johannesburg
 - Cape Town
 - Other
3. Are you aware that your personal data is being gathered, analysed, and stored by various companies and used to personalise marketing messages?
 - Yes
 - No
4. Has a company ever acquired your data without your permission that you know of or suspect?
 - Yes
 - No
5. Has a company ever mishandled your personal data?
For example, sold it to another company without your permission.
 - Yes
 - No
 - Unsure
6. Do you accept to be potentially contacted for a more in-depth interview about this topic?
 - Yes
 - No

Open Ended Interview

1. What do you consider to be an invasion of digital privacy?
2. How do you feel when you encounter such actions from digital marketing activities?
3. In your opinion, do you feel that you have control over your personal information when engaging with online brands? Please explain how this control, in your opinion, is or isn't impacted by brands.
4. How do you generally feel about digital marketing activities that require the sharing of personal data?
5. Are there any specific activities that you feel comfortable with or uncomfortable with?
6. Can you describe any instances where you have felt that your privacy was compromised by digital marketing activities? What specific activities do you believe were responsible for this?

7. How important is trust when it comes to engaging with online brands? Please explain why you say so.
8. Have you ever had an experience where invasive data gathering negatively impacted your trust in a brand or organisation?
9. Can you describe this experience and how it affected your relationship with the brand?
10. How did their actions impact your perception of digital marketing activities in general?
11. What steps do you believe organisations should take to help minimise privacy concerns when engaging in digital marketing activities? Are there any specific practices or guidelines that you think should be followed?
12. How do you think data privacy will change in the future?
13. Do you have any other thoughts on the topic you would like to share?

Annexure C: Ethical Clearance Letter

Data Classification - Business General



28 June 2023

Student name: Elke Stegmann
Student number: [REDACTED]
Brand and campus: Vega Online



Approval of BCom Honours in Strategic Brand Management Proposal and Ethics Clearance



Your research proposal and the ethical implications of your proposed research topic were reviewed by your supervisor and the campus ethics committee, a subcommittee of The Independent Institute of Education's Ethics Committee.



Your research proposal posed no significant ethical concerns and we hereby provide you with ethics clearance to proceed with your data collection.



There may be some aspects that you still need to address in your proposal. If this is the case, feedback will be provided to you in writing. You will need to address these aspects in consultation with your supervisor.

In the event that you decide to change your research topic or methodology in any way, kindly consult your supervisor to ensure that all ethical considerations are adhered to and pose no risk to any participant or party involved. A revised ethics clearance letter will be issued in such instances.

We wish you all the best with your research!

Yours sincerely,



Dr Tish Taylor
Supervisor



Dr Tish Taylor
Chair of the Campus Ethics Committee

ADVTECH House: Inanda Greens, 54 Wierda Rd West, Wierda Valley 2196
P.O. Box 2369, Randburg 2125

Directors: RJ Douglas (UK), JDR Oesch, MD Aitken, SCD Lurie
Group Company Secretary: CB Crouse



The Independent Institute of Education (Pty) Ltd is registered with the Department of Higher Education and Training as a private education institution under the Higher Education Act, 1997 (reg. no. 2007/HED/002). Company registration number: 1987/004754/07.

© The Independent Institute of Education (Pty) Ltd | ADVTECH Resourcing | ADVTECH LTD

Annexure D: Concept Document

<u>Project details</u>	
Your Name: Elke Stegmann	Student Number: [REDACTED]
Supervisor: Tish Taylor	Date: 20/11/2023 Version: 6
<u>Proposed Title</u>	
Title	Privacy in the Digital Age: Understanding the effect of privacy invasion on South African consumers' brand trust.
<u>Research details</u>	
Problem statement	Massive amounts of consumer data are collected, analysed, and stored for digital marketing purposes (Wang & Baker, 2022), frequently without the consumer's full awareness or understanding (Martin & Murphy, 2017). This has diminished the understanding of and respect for digital privacy and the violation thereof. Yuvaraj and Indumathi (2018) state that digital marketing activities are an extension of brand building, which means that any feelings consumers have towards digital marketing activities, will be transferred to the brand as well. Additionally, Kelly, Kerr, and Drennan (2017) found that consumers' trust in brands has decreased in the digital space due to the reasons stated above. Kelly <i>et al.</i> (2017) state that consumers have more trust in technology than they do in the brands communicating with them using this technology. The problem is that consumers are being affected by unethical digital marketing activities and that possibly hurts brand trust.
Purpose statement	The purpose of this study is to understand how consumers are affected by invasive data gathering techniques – specifically for digital marketing purposes – and how this has impacted their trust in and relationship with brands.
Research question/s	Primary: 6. How does online data gathering, driven by digital marketing activities, impact on consumer relationships and brand trust? Secondary: 7. When do consumers perceive data gathering to be an invasion of digital privacy? 8. How is the success of digital marketing and online brands impacted by this experience with privacy invasion? 9. How is the control of consumers over their information affected by digital marketing activities? 10. How does the experience of consumers affect their trust in and relationships with brands?
Hypotheses / Objectives	1. Determine which digital marketing activities affect consumer privacy.

	2. Understand the attitude of consumers towards these digital marketing activities. 3. Determine how much control consumers have or had over their data. 4. Determine how organisations can help minimise or solve privacy concerns. 5. Understand how invasive data gathering affects South African consumers' trust in and relationship with brands.					
Research rationale	Ashworth and Free (2006) state that digital marketing technology has and continues to evolve at a rapid pace, and with it, privacy concerns grow. According to Martin & Murphy (2017), relevant academic materials have not evolved as rapidly as marketing technology and marketers' use of consumer data, limiting the reliable information that is available on the topic. This rapid development of marketing technology combined with the need for highly detailed and personal consumer information to be successful has led to unfair and in some instances even aggressive data-gathering and digital marketing techniques that result in customer suspicion and frustration (Mandal, 2019). Additionally, consumers feel ill-equipped to regain or stay in control of their personal information due to a lack of knowledge regarding the technology and complex privacy policies (Albulayhi & Khediri, 2022). Wang (2018) found that consumers' privacy concerns regarding digital marketing had a predominantly negative effect on their trust in brands which ultimately had a negative impact on the consumer-brand relationship. There is a gap in the understanding of the effects data gathering and loss of ownership over data have on consumers' trust in and relationships with brands. This study aims to lessen that gap by shedding light on the technology and practices that are truly invasive, how consumers are affected by this invasion, and how their trust is consequently affected.					
Literature overview						
Key theories	1. Privacy. The theory is defined using a multi-definition approach. These include privacy as control, power, trust, obscurity, and contextual integrity. 2. Brand trust. Theorised by breaking a definition of brand trust down into two components, namely, brand reliability, and brand intention					
Seminal authors/sources	Alan Westin (1967), Selinger and Hartzog (2014), Ari Waldman (2015), Richards and Hartzog (2017), Carissa Véliz as cited by Wilsdon (2022), Nissenbaum, (2004), Delgado-Ballester, Munuera-Alemán, and Yagüe-Guillén (2003)					
Literature review themes	<u>Theme 1</u> Ways consumer privacy is affected.	<u>Theme 2</u> Attitudes of consumers	<u>Theme 3</u> Consumer control over personal data	<u>Theme 4</u> Effect of privacy invasion	<u>Theme 5</u> How organisations can solve privacy problems	<u>Theme 6</u>
Sources	Ashworth & Free (2006), Albulayhi & Khediri (2022), Wahyuningtas (2017), Martin & Murphy (2017), Bandara, Fernando, & Akter (2020), Pike (2020), Engels (2019), Richard & Hartzog (2017), Turrecha & Ashley (2021), Wieczorkowski & Polak (2017). Journals of law, market research, marketing management, consumer studies, business ethics, interactive mobile technologies, marketing science, and applied knowledge management.					

Key concepts	Personal data/information, data governance and data protection, privacy violation, marketing technology
--------------	---

<u>Provisional Research Approach</u>				
Paradigm	<u>Paradigm</u> Interpretivism	<u>Epistemology</u> Interpretivism	<u>Ontology</u> Interpretivism	<u>Axiology</u> Interpretivism
Approach/ design	This was a qualitative study. Qualitative research typically relies on words and data based on meaning rather than numerical and statistical data (Maree, 2019). This study purely focused on words and meaning derived from data which is why I have chosen a qualitative approach. An inductive line of reasoning is used with a cross-sectional time dimension. This was an exploratory study. When a research topic focuses on an unexplored or new area, it is an exploratory study (Swedberg, 2020). Understanding the effects of privacy invasion on brand trust remains an under-researched topic.			

<u>Provisional Research Plan</u>	
Population	Target population: Consumers who have been affected by invasive digital marketing practices in some way. Accessible population: South African consumers living in Johannesburg or Cape Town between the ages of 30-50 who have been affected by invasive digital marketing activities in some way.
Sampling	Purposive and snowball sampling will be used for this study. According to Maree (2019), purposive is used when there is a specific purpose behind the sampling method. In this case, there is the specific purpose of sampling individuals who have already been affected by invasive data gathering
Data collection method(s)	Semi-structured interviews. Semi-structured interviews are used when the researcher has already created a line of inquiry (Maree, 2019). The interview consists of some open-ended questions which leave room for some expansion from participants (Maree, 2019). This will be an appropriate method for this study because it will give me a clear insight into the experience of each individual respondent, it will not be closed off answers with no room for individuality.
Data analysis method(s)	Narrative analysis. According to Maree (2019), this analysis method extracts meaning from narratives which are created during data collection. I will extract meaning from the narratives and stories told by the participants of my semi-structured interviews.

<u>Ethical considerations and limitations</u>	
Ethics	Ethical considerations for this study are vast. It is an ethically sensitive topic and bias is involved in answering the questions. Because of this, no questions will be asked in a manner that could sway participants' way of answering them. Consent with full knowledge of all factors involved in this research project and how the data will be used is required before any participant can partake. Participants will be made aware of their full right to withdraw from the study at any given time. They are also in their right and will be made aware of it, that they do not have to answer certain questions, or they can answer them as detailed or undetailed as they like. The interviewer will under no circumstances request them to elaborate if they stated they would prefer not to. Participants are allowed to bring forward any concerns at any given point and they will be dealt with by the researcher in an appropriate manner.
Limitations	A lack of research done on the concept of digital privacy in the South African context. There is also less research that specifically relates to digital marketing's effect on digital privacy than there is on just digital privacy. This makes gathering literature difficult.

Annexure E: Research Questions

Primary:

1. How does online data gathering, driven by digital marketing activities, impact on consumer relationships and brand trust?

Secondary:

2. When do consumers perceive data gathering to be an invasion of digital privacy?
3. How is the success of digital marketing and online brands impacted by this experience with privacy invasion?
4. How is the control of consumers over their information affected by digital marketing activities?
5. How does the experience of consumers affect their trust in and relationships with brands?