Re-Examining Privacy Conceptualisation in the Context of Online Behavioural Advertising

A thesis presented in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in

Marketing

at Massey University, Wellington

New Zealand

Jiaqi Zhu

2025

Abstract

This PhD thesis challenges dominant assumptions about consumer privacy in Online Behavioural Advertising (OBA). While most research defines privacy as "control," this study critically asks whether that concept, and the findings built on it, actually reflect how people experience privacy online. Accordingly, the thesis addresses the overarching research question: *Has consumer privacy been validly conceptualised in the context of OBA? If not, what are the theoretical and empirical implications of this conceptual inadequacy for privacy research in OBA?*

Grounded in *critical scientific realism* (Niiniluoto, 1999), the thesis aims to examine whether privacy theories and empirical evidence in OBA are *cognitively successful,* that is, whether they offer a true representation of reality (Niiniluoto, 1999). Through critical examinations of key privacy conceptualisations, theories and research in OBA, the thesis argues that much of the existing research lacks cognitive success. Specifically, privacy as "control" fails to achieve cognitive success in capturing individual heterophenomenological cognition of privacy experience (Dennett, 2007), while also neglecting privacy's social value (Hull, 2015). But the problems don't stop at definitions. This thesis also exposes key theoretical cracks in the empirical foundations. A critical examination reveals four core issues undermining the coherence of the empirical findings: the confounding contextual variables, the

misspecification of cognitive appraisal variables, the missing trade-offs, and the shaky mediator.

While offering cognitively successful solutions, the thesis delivers three major contributions: (1) it reconceptualises privacy as a state, capturing the psychological nature of how people experience privacy today, while highlighting privacy's social value; (2) it synthesises and critiques fragmented empirical findings to expose deeper theoretical problems, serving as a template and encouragement for other researchers to present robust critiques of privacy in OBA; and (3) it introduces the Contextual Privacy State model, a novel framework that offers a more realistic and scientifically grounded understanding of privacy in digital environments. Together, these contributions push privacy research toward greater theoretical rigour and cognitive success.

Acknowledgments

First and foremost, I would like to extend my deepest gratitude to my main supervisor, Dr. Mark Avis. From my initial research into *Consumer Privacy Concerns and their Adaptation to Online Behavioural Advertising* to the final thesis on *Re-examining Privacy Conceptualisation in the Context of Online Behavioural Advertising,* it has been Mark's rational thinking, critical mindset, and educational philosophy that have sparked a truly exhilarating intellectual journey. Under his guidance, I have come to appreciate the power of theory and critique not just in academia, but in life and work.

I am equally grateful to my co-supervisor, Dr. Vishnu Menon. I completed my PhD confirmation in November 2021, during the height of COVID-19, amid Massey's financial difficulties and reconfiguration. Before settling into the Wellington campus, I faced the possibility of changing my main supervisor, a situation that could have significantly reshaped my research topic. At the time, I had little academic footing and was overwhelmed by the cultural, environmental, and emotional upheaval of moving to another country. Vishnu's steady presence, patient encouragement, and detailed academic guidance helped me build my scholarly mindset, piece by piece, while also easing my transition into life in Wellington.

I would also like to thank Massey's School of Communication, Journalism, and Marketing, and the Centre for Learner Success, for offering me opportunities to work as an assistant lecturer and a pre-reading consultant. These roles provided me with firsthand experience of New Zealand's university management systems and workplace culture. They also sharpened my intercultural competencies and enriched my CV. Beyond academia; I had the privilege of founding and leading the Wellington Chinese Postgraduate Association and the Massey Wellington Chinese Students Association. I am immensely grateful to the various New Zealand government bodies and non-profit organisations that invited me as a guest or volunteer to participate in bilateral events spanning culture, education, trade, and tourism. These experiences impressed upon me the importance of navigating both global and local insights, and of understanding oneself as part of broader political and economic flows.

To the mentors I met at professional and social events across academia, business, and politics: thank you for lifting me with your encouragement and support. To my PhDers in the CJM office, you were more than colleagues; you were friends, therapists, and allies. To my Wellington friends, thank you for trusting me and supporting me. And to my lifelong friends back in China: thank you for being my emotional anchors, for the seamless transportation, and for promising me Haidilao upon my return.

I would like to thank my father, Mr. Xulong Zhu, and my mother, Mrs. Xiaohong Yao, for their unwavering belief in the value of education. Even knowing that educational investment yields the slowest return, they never hesitated to support me financially, intellectually, and emotionally. Thank you for being my parents, and for giving me both a home and unconditional love.

My PhD journey has come to a close, but I leave not just with a degree, but with growth, insight, and a renewed sense of purpose.

May the future carry this wish:

“To establish moral consciousness in the universe;

To secure life for the people;

To revive extinct doctrines of ancient sages;

To create lasting peace for generations to come.”

Table of Contents

List of Figures

List of Tables

List of Abbreviations

OBA: Online Behavioural Advertising

CPS: Contextual Privacy State Model

APCO: Antecedents-Privacy Concerns-Outcomes (APCO) Model

CFIP: Integrative framework on Concerns for Information Privacy

SMP: Social Media Privacy Model

PPM: Privacy Process Model

Chapter 1: Introduction

1.1 Background to the Research

As the digital world has become increasingly ubiquitous in consumers' everyday lives, interest in consumer online privacy has grown significantly. With the broader context of online technologies development, consumer privacy concerns continue to play an integral part in influencing customer fears and loyalty of online retailing in e-commerce (Liyanaarachchi, 2020), and are pertinent to the smartphone applications usage (Maseeh et al., 2023). In the case of online advertising, concerns about individual privacy have moved from a peripheral issue to a central question from the perspective of consumers (Palos-Sanchez et al., 2019), organisations (Nill & Aalberts, 2014), and society (Scott, 2013), particularly since the early 21st century. As such, research on consumer privacy within online advertising has rapidly expanded, forming a wide body of literature.

Against this broader backdrop, online behavioural advertising (OBA) represents a particularly salient context, which saw the proliferation of privacy research from all perspectives, especially consumers. In 2001, OBA began to be implemented in commercial practice after Google rediscovered the value of its users' online behavioural data and applied it to match online advertising. OBA refers to "the tracking of users when they surf the Internet and the building of profiles over time, which are later used to provide them with advertisements matching their interests"

(Article 29 Data Protection Working Party, 2010, p.3). Users' online behavioural data may include "web browsing data, search histories, media consumption data (e.g., videos watched), app use data, purchases, click-through responses to ads, and communication content, such as what people write in e-mails (e.g., via Gmail) or post on social networking sites (Boerman et al., 2017, p. 364)." A classic example is a consumer who searches for flights to New York on one website, and then, while browsing unrelated content elsewhere (e.g. newspaper's website), is shown advertisements for the same route (Federal Trade Commission, 2009). It is apparent from the example that at the heart of the OBA operational process is the aim of accumulating large amounts of information about consumers' online activities and using them to individually target ads (Boerman et al., 2017).

Since then, OBA has grown into one of the most prevalent and controversial practices in digital marketing (Boerman et al., 2017; Zuboff, 2019). On the one side, OBA has become a powerful commercial marketing tool within the advertising industry, due to its exceptional ad revenue and market capitalisation, such as higher click-through rates and improved return on investment (Matthewson, 2006; Zuboff, 2019). On the other side, consumers have accused OBA of violating their privacy. In particular, consumers frequently expressed that OBA's operational processes of data collection, profiling, and data usage as privacy-invasive. Research indicated that consumers commonly express concerns about the potential misuse of their personal data, the

receipt of unwanted advertisements, data security risks, and the discomfort of manipulation (Smit et al., 2014).

In response to the growing consumer privacy concerns, countries have made substantial advances in the governance and protection of consumer privacy in OBA. These efforts include the establishment of national independent OBA advisory bodies, the announcement of self-regulations (Borgesius, 2013; Martin & Durphy, 2017), the updating of relevant mandate programs (informed opt-out and opt-in consents) (Borgesius, 2013; Martin & Durphy, 2017), the supervision of advertising companies (An et al., 2018; Eijk et al., 2012), the academic scrutiny and evaluations of regulations, programs, and policies (Altman et al., 2011; Martin & Murphy, 2017; Scott 2013; Smit et al., 2014).

Alongside these regulatory and institutional developments, academic research focusing on consumers' privacy concerns in OBA also saw a growing proliferation. Besides legal and law studies, scholars have conducted a wide range of empirical studies exploring consumer privacy concerns, seeking to understand their conceptual and operational processes. That is, the conceptualisation of what privacy *is*, and how it is empirically experienced. Nonetheless, as will be introduced in the follow-up sections, despite this growing body of empirical work, how consumer privacy is conceptualised and operated in OBA remains contested.

1.1.1 Consumer Privacy Conceptualisation in OBA

The question of what privacy is has long been a central focus of scholarly research. In the majority of studies in the fields of information systems and marketing, privacy is typically conceptualised as information privacy. Information privacy refers to who gathers and disseminates information under which circumstance (Li, 2011; Smith et al., 1996; Westin, 1968). Central to this conceptualisation is the notion of individual control over information transactions involved in data gathering and usage, e.g., monitoring, collecting, storing, and analysing (Palos-Sanchez, 2019; Smit et al., 2014). These attributes of information privacy reflect what Smith et al. (2011) describe as the "privacy as control" conceptualisation approach, whereby privacy is defined in terms of individuals' control over information in much of the prior literature.

OBA, as an online marketing tool whose operation relies on information gathering and usage, also defines consumer privacy as information privacy. Within the dominant body of OBA privacy literature and research, consumer privacy is predominantly conceptualised in terms of consumers control over their online behavioural information- that is, concerns regarding who gathers and disseminates their information under the circumstance of OBA (Baek & Morimoto, 2012; Bleier & Eisenbeiss, 2015; Gironda & Korgaonkar, 2018; Ham, 2017; Jung, 2017; Kim & Huh,

2017; Li, 2011). This conceptualisation approach reflects a broader tradition in the conceptualisation of information privacy. Accordingly, much of the OBA privacy literature follows the "privacy as control" approach.

However, when reviewing the large body of OBA privacy literature, recent empirical findings suggest that consumer responses to OBA often go beyond control-based approach but transition to a state-based approach. Studies show that consumers often describe privacy intrusions not just in terms of lost control, but as emotional reactions, such as feelings of creepiness, intrusion, and violation (Aguirre et al., 2015; Phelan et al., 2016). It is apparent that these emotional responses are not easily captured by the control-based approach, but Smith et al's (2011) state-based approach, which views privacy as a state of limited access (to a person, to situations, or to information). This signals the need for a deeper conceptual rethink through the lens of Smith et al's (2011) privacy conceptualisation categorisation.

This thesis argues for a conceptual transition from control-based to a state-based conceptualisation of privacy. Such a shift addresses longstanding calls for more psychologically grounded perspectives on privacy, drawing on insights from social (Hunt, 2003) and personality psychology (Stuart et al., 2019). Yet, as Brown (2002) notes, definitions play a critical role in shaping marketing theory and practice. Therefore, any redefinition of privacy must rest on solid theoretical and empirical

foundations. This thesis will contribute to that effort by critically examining the prevailing control-based conceptualisation and making the case for reconceptualising consumer privacy as a state, which is subsequently examined through empirical investigation.

1.1.2 Consumer Privacy Empirical Evidence in OBA

Beyond the question of *what privacy is*, OBA scholars have increasingly sought to understand how privacy is experienced empirically by consumers. This interest is reflected in the proliferation of empirical studies on consumer privacy concerns. These studies largely focus on identifying the factors that shape such concerns and examining how they influence both the effectiveness of OBA and consumer behaviour.

Privacy concerns have been explored extensively as antecedents (Boerman et al., 2017; Gironda & Korgaonkar, 2018; Ham, 2017; Smit et al., 2014), outcomes (Brinson et al., 2019; Kim & Huh, 2017; Mpinganjira & Maduku, 2019), and moderators (Noor et al., 2019; Zarouali et al., 2017). However, despite this growing body of work, as it will be argued later in Chapter 3, empirical findings remain fragmented and often inconsistent, particularly with respect to the relationships between antecedent factors, consumer privacy concerns, and outcome variables (see Table 2 in Chapter 3 for an overview).

For instance, while some studies have found a correlation between perceived benefits and a reduction in privacy concerns (Ham, 2017), others find the opposite result which reports that increased perceptions of usefulness actually heighten such concerns (Jung, 2017; Palos-Sanchez et al., 2019). Similarly, while privacy concerns are frequently used as predictors of their willingness to click on or engage with an advertisement (Bleier & Eisenbeiss, 2015), this effect has not been found in other studies (Gironda & Korgaonkar, 2018; Kim & Huh, 2017). These inconsistent findings may have contributed to an ongoing lack of clarity regarding the precise role and function of consumer privacy concerns within OBA research.

This lack of consistency raises a fundamental question: what explains these fragmentations and inconsistencies in empirical findings? Are they the result of conceptual ambiguity, hypothesis misspecification, theoretical fragmentation, or a deeper misalignment between how privacy is theorised and how it is operationalised? To address this question, this thesis undertakes a critical literature review of the empirical studies on consumer privacy in OBA, with the aim of uncovering underlying patterns, gaps, and theoretical blind spots.

In the comparable domains, such as social media (Trepte, 2021) and e-commerce platforms (Maseeh, et al., 2021), they have consolidated numerous empirical findings into integrative frameworks seeking to find how consumer privacy operate in the specific domain. For example, Trepte (2021) proposed a general privacy framework for social media that integrates the effects of individual assessments with social media boundary conditions on the subjective experience of privacy and privacy behaviour. Through a meta-analysis of a wide range of privacy studies, Maseeh et al. (2021) proposed and tested a framework in which consumers' perceived irritation influences their intention to receive mobile advertising through their attitudes toward online advertisements. However, comparable integrative efforts that systematically synthesise empirical evidence into theoretical frameworks (or further empirically test such frameworks) remain largely absent in the OBA privacy literature, despite the centrality of privacy concerns to the academic discourse in this space (Boerman et al., 2017).

In light of this gap, the present thesis asks: Can the existing body of empirical evidence, once subjected to critical examinations, serve as a sufficient foundation for constructing a coherent, comprehensive model of consumer privacy in OBA? To this end, the thesis proposes to move beyond fragmented empirical interpretations and instead develop a generalisable model that reflects the consistent and clarified nature of privacy experiences in OBA.

1.2 Research Question

Given the two trends discussed in the background section, this research seeks to answer the following overarching question: *Has consumer privacy been validly conceptualised in the context of OBA. If not, what are the theoretical and empirical implications of this conceptual inadequacy for privacy research in the context of OBA?*

There are two elements to this overall research question. The first is to clarify whether consumer privacy has been validly conceptualised. The second element is rooted in the critical analysis of privacy empirical research in OBA. Both elements are grounded in *critical scientific realism* (Niiniluoto, 1999). It is a philosophy which, as Hunt (2003) suggests, includes the perspective that theory and research should be critically evaluated and tested to determine the extent to which they do, or do not, truly correspond to the world. Therefore, guided by the central research question, this project, grounded in *critical scientific realism* (Niiniluoto, 1999), adopts a critical approach to re-examining the key privacy conceptualisations, theories and research in OBA to uncover the issues behind them.

1.3 Theoretical Nature: Philosophical Foundations

Given the conceptual rethink and empirical examinations, this thesis is *theoretical* in nature. The philosophical foundation of this thesis is the *critical scientific realism* (Niiniluoto, 1999). It is a philosophy whose concept of verisimilitude is that theory, although it may go beyond the limits of empirical observation, needs to be a description of reality, and that observations, measurements and experience must interact with that reality (Niiniluoto, 1999). He argues that:

A theory should be *cognitively successful* in the sense that the theoretical entities it postulates really exist and the lawlike descriptions of these entities are true. Thus *the basic aim of science for a realist is true information about reality*. (Niiniluoto, 1999, p.167)

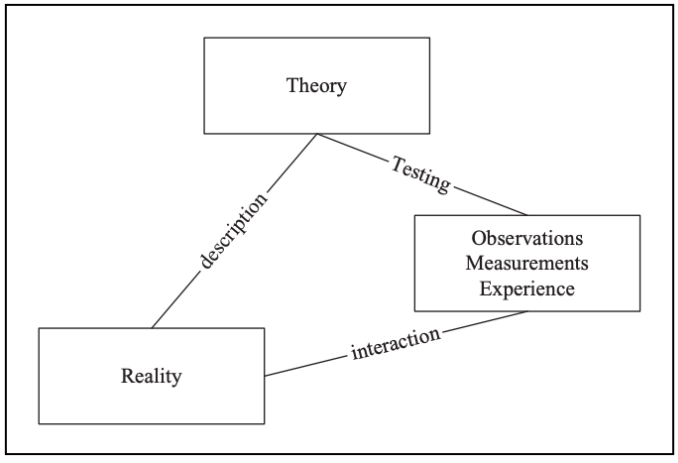


Figure 1. *The Interaction of Reality, Theory, and Empirical Evidence*

Niiniluoto (1999) recognises that people have their own understanding of the world, while Dennett (1993) further argues that such mental perceptions must be considered "real", regardless of whether the world itself is "real". For example, people's perceptions of understanding work of an "unreal" fiction are "real" in the sense that they really exist and can therefore be studied scientifically.

In the case of consumer privacy, this implies that theoretical entities (e.g., privacy concepts, research, and frameworks) should aim to describe the reality of consumers' mental perceptions of privacy. As discussed earlier, existing studies have proposed multiple and sometimes divergent understandings of consumer privacy in OBA. For example, much of the OBA research conceptualises consumer privacy through perceptions of information control (Baek & Morimoto, 2012; Bleier & Eisenbeiss, 2015; Gironda & Korgaonkar, 2018; Ham, 2017; Jung, 2017; Kim & Huh, 2017; Li, 2011). However, other studies examine consumer privacy in OBA as emotional reactions, focusing on feelings of creepiness, intrusion, and violation (Aguirre et al., 2015; Phelan et al., 2016).

These multiple research findings reinforce a long-standing argument that privacy research facilitates numerous conceptual threads that have yet to be woven into a cohesive fabric. However, grounded in *critical scientific realism*, it becomes possible

to identify which consumer perceptions of privacy can be regarded as more “real” and “scientific” in describing their understanding of privacy in OBA.

1.4 Significance

Examining consumer privacy at a theoretical level is of high significance. As Marketing is often acknowledged as a *practical* discipline (Martin & Murphy, 2017), it tends to overlook the importance of *theoretical scientific realism* (Hunt, 2003). This oversight becomes particularly salient in the digital age, where consumer privacy concerns are deeply intertwined with Online Behavioural Advertising (OBA), an emerging, technology-driven form of online personalised advertising (Boerman et al., 2017).

This absence of critical evaluations has resulted in numerous conceptual threads in privacy. This raises a fundamental concern: whether current privacy output in OBA produces true information about consumer perceptions, or merely generates fragmented and conceptually inconsistent findings. Consequently, consumer privacy research risks continuing to rely on conceptualisations that do not validly represent the reality of consumer perceptions in the OBA context, while empirical findings derived from such conceptualisations may remain fragmented and inconsistent, thereby limiting their cumulative contribution to knowledge development.

As Avis et al. (2012) argue, theoretical explanations must clarify why particular concepts are relevant for explaining consumer perceptions. In the case of privacy in OBA, theory should be able to explain why consumers may experience privacy either as a matter of information control or as feelings of intrusion. However, to the best of my knowledge, no existing PhD research on privacy in OBA has examined whether the numerous current academic outputs, including conceptualisation, theory, and empirical findings, are *cognitively successful* in explaining consumer perceptions. Instead, the field has largely proceeded by accumulating empirical outputs of consumer privacy without critically evaluating whether these outputs provide a true representation of consumer perpections in the OBA context.

This urgent gap calls for a *cognitively successful* study, one that rigorously examines the scientific realism of privacy conceptualisation and empirical findings in OBA. Addressing this need constitutes the first key significance of this thesis. This PhD research lies in its capacity to clarify which conceptualisations and theoretical explanations meaningfully account for consumer privacy perceptions in OBA. Through critical examinations of prior privacy research in OBA, this thesis identifies the root causes of existing studies' failure to achieve cognitive success, and proposes and tests scientifically grounded privacy conceptualisations together with a

theoretically coherent privacy model. In doing so, the study contributes to establishing a clearer and more coherent theoretical foundation for future privacy research.

Beyond its theoretical contributions, clarifying the conceptual foundations of consumer privacy also carries broader practical significance. When privacy research is grounded in theoretical explanations that more accurately represent consumer perceptions, the knowledge generated becomes more capable of informing practice. In the context of OBA, where regulatory debates and managerial decisions frequently rely on insights from academic research, conceptually robust and cognitively successful theories are essential for providing reliable guidance. By strengthening the theoretical foundations of privacy research through a critical scientific realist perspective, this thesis contributes to producing knowledge that is not only theoretically meaningful but also more capable of informing practical and managerial implications in industry.

1.5 Methodological Approach and Outline of the Research

As Hunt (2003) considered, "A fundamental tenet of scientific realism is that it is *critical*. That is, all knowledge claims must be critically evaluated and tested to determine the extent to which they do, or do not, truly correspond to the world (p. 292)". This means that the *critical scientific realism* could be approached through

conceptual review. Therefore, this thesis centres on a critical examination of privacy research within OBA.

Throughout much of this thesis, I undertake critical examinations of privacy conceptualisations, theories and research in OBA, although empirical research is also included to support some of the conceptual reviews. The approach to examining the consumer privacy research throughout the thesis can be summarised as follows:

1. Review and critical examination of privacy conceptualisations from perspectives of definitions and measurements used in OBA.

2. Review and critical examination of consumer privacy empirical evidence in OBA and privacy models built upon in empirical tradition.

3. Develop a new privacy model based upon above theoretical examinations.

Accordingly, the chapters are organised through literature reviews, critical evaluations, empirical research, and/or the development of theoretical solutions. The central research question is resolved through different chapters, summarised as follows:

Chapter 1 builds the contextual foundation of the thesis by introducing the research background, research questions, contributions, and the thesis structure. Chapter 2 reviews how consumer privacy has been defined and measured in OBA literature, noting the dominant framing of privacy as control. Chapter 3 reviews existing empirical research on consumer privacy in OBA and conducts an inductive thematic analysis of 99 studies within this body of work. It subsequently identifies the fragmented and inconsistent patterns within the current empirical evidence.

Chapter 4 offers a critical appraisal of previous conceptualisations and measurements of privacy, advancing the notion of privacy as a state and supporting it through theoretical argumentation. Chapter 5 critically evaluates prior empirical findings, drawing attention to key theoretical issues such as the role of confounding contextual variables, mis-specified cognitive factors, and neglected trade-offs. Chapter 6 evaluates existing privacy models to determine whether they address the theoretical and empirical shortcomings identified earlier. Finding persistent gaps, it underscores the need for a new conceptual framework.

In Chapter 7, the thesis turns to its empirical component. A mixed-methods study is undertaken, involving primary data collection through interviews and an online questionnaire, to empirically test the viability of conceptualising privacy as a state.

The findings demonstrate that consumers experience privacy as a state intuitively and reasonably in response to OBA.

Chapter 8 introduces the Contextual Privacy State (CPS) model as a theoretically grounded solution, offering a more comprehensive understanding of consumer privacy in OBA and other privacy contexts. Chapter 9 concludes the thesis by summarising key findings, contributions, and future directions.

1.6 Contributions

While this thesis contributes methodologically by employing a mixed-methods approach to access privacy as a state, which contributes to methodology development, its most significant contributions lie in advancing *theoretical scientific realism* by offering a true representation of privacy in OBA and the broader privacy landscapes. Specifically, a transition to define privacy as a state and the development privacy model.

The overall conclusion is that the conceptualisations of privacy as a right, a commodity, and a control are not cognitively successful. That is, they are not coherent and do not describe the reality of individual privacy. The critical review of these three conceptualisation streams finds that it is apparent that (1) the core problem of privacy

as a right is that it does not define what privacy *is* before arguing whether this is something people should have a right to; (2) the problem with privacy as a commodity is that it does not say what the commodity actually is and also metaphor privacy as commodity is not literature accurate (Cornelissen, 2003); and (3) privacy as control is theoretical tenuous as individuals cannot possess efficient control over their information in the digital age and overemphasis economic rational neglecting privacy's social significance. Nevertheless, the conceptualisation of privacy as a state better represents the reality of privacy. It is proposed that conceptualising privacy as a state has potential for greater cognitive success in describing individual heterophenomenological cognition of privacy experience (Dennett, 2007) and presents social value (Hull, 2015), and the transition of defining privacy as a state is the first contribution of this thesis.

The second contribution of the thesis is to commerce the critical analysis of the empirical research on consumer privacy concerns in OBA. In highlighting the role of privacy concerns in privacy behaviour in OBA, the overview of the empirical research reveals fragmented antecedents and outcomes of privacy concerns and inconsistencies in findings alongside them. The further work of this thesis exposes four underlying theoretical issues underlying the fragmentations and inconsistency, that is, the confounding contextual variables, the misspecification of cognitive appraisal variables, the missing trade-offs, and the shaky mediator. An overview of empirical

evidence represents an important starting point for synthesising results in order to have a big-picture understanding of the research progress. Critically examining the results, therefore, represents a contribution to narrowing down the underlying and obvious issues. In combination, the critical analysis of empirical research on consumer privacy concerns in OBA can serve as a template and an encouragement for other researchers to present robust critiques.

The final contribution of this thesis is the development of the Contextual Privacy State (CPS) model, which is a valid critical framework for understanding consumer privacy in OBA and broader privacy field. By defining privacy as a state and emphasising the centrality of trade-offs, this model draws upon the critical analysis of privacy conceptual and empirical issues identified previously. The model also has drawn extensively on prior privacy models but sought to avoid each of the flaws highlighted in another critical examination of privacy models. As such, the CPS model is a perfect product of the critical scientific realism (Niiniluoto, 1999), and therefore, it serves as a true representation of the reality of the operation of individual privacy at least from the theoretical perspective.

1.7 Summary

This chapter has outlined the inspiration for the research question, clarified the research question, and provided a framework for the thesis's structure and approach to addressing the research question. This thesis identifies the importance of critical analysis regarding privacy concepts and empirical research in studying consumer privacy concerns in the OBA. Furthermore, it proposes the Contextual Privacy State (CPS) model as a novel approach to resolving the highlighted through the critical analysis.

Chapter 2: Privacy Conceptualisation in OBA – Literature Overview

2.1 Introduction

To address the first notable issue raised in the background - namely, the consumer privacy conceptualisation, this chapter examines how privacy has been framed in the OBA literature, focusing on both definitions and measurement approaches. It begins by tracing the evolution of privacy definitions and explores why the "privacy as control" has become the dominant conceptualisation in OBA research. It then reviews the key measurement instruments used in empirical studies, revealing a strong alignment with this control-based approach. By uncovering these definitional and methodological patterns, the chapter lays a foundation for deeper critical theoretical analysis in the chapters that follow.

2.2 The Importance of Definitions

The issue of definition is central to conceptual clarity across marketing fields. As Brown (2002) argues, the marketing field is rife with "ethereal, overarching, ill-defined, pseudo-philosophical concepts (p. 320)", which can create significant theoretical and practical challenges. MacKenzie (2003) further highlights those poor definitions lead to multiple issues, such as deficient measures, measurement model misspecification, and weak theoretical rationale for hypotheses.

These issues are prevalent in marketing research. For example, Avis and Henderson (2022) found that an increasing number of brand-related concepts caused a lack of clarity in definition, making the brand concept opaque and unwieldy. Similarly, Stern et al. (2001) pointed out that the ambiguous utilisation of the same term "image" for different phenomena had given rise to deficient measurements in brand, corporate, and store image research. Expanding on this, Stern (2006) criticised idiosyncratic brand definitions, noting that these caused researchers to study different concepts under the same name or the same concept under different names. It is apparent that a lack of a clear (and agreed) definition can translate into a disarray of definitions, research challenges, and barriers to practical application and theoretical development.

The consequences of such definitional ambiguity go beyond brand, impacting the study of privacy as well. Without a clear, agreed-upon definition, privacy research risks becoming fragmented, leading to disarray of definitions, measurement inconsistencies, and theoretical confusion. Given these challenges, it is crucial to review and examine how privacy, particularly in the context of OBA, has been defined and measured in existing literature.

In light of these concerns, the following sections review definitions and measurement approaches related to privacy in OBA research. By doing this, this thesis aims to

identify key theoretical trends of privacy within OBA and lay the groundwork for later critical examinations.

2.3 Privacy Definitions in OBA

Given that consumer privacy research in OBA heavily relies on previous definitions of privacy, a review of these foundational definitions offers valuable insights into the understanding of consumer privacy in the OBA context.

2.3.1 The Evolution of Privacy Definitions and Types

One of the earliest and most influential definitions of privacy is the notion of a "right to be left alone" (Warren & Brandeis, 1890). This definition, which has become ubiquitous in legal and political discourse (Smith et al., 2011), is often criticised as a broad, catch-all term subsumed under societal ethics and moral values (Smith et al., 2011). Although this definition is often regarded as the first general conceptualisation of privacy, it has been challenged due to the rise of information technology (IT) and its application to consumer behaviour. Scholars argue that IT has complicated the boundaries of this "right," particularly in light of the privacy paradox observed in consumer behaviour studies: despite high reported privacy concerns, consumers often share personal information in various contexts (Awad & Krishnan, 2006). This paradox further calls into question the adequacy of the "right to be left alone" in explaining contemporary privacy issues (Smith et al., 2011).

The ongoing contestation of privacy as a right led subsequent theorists to reconsider privacy within the context of technological advancements, especially in computer and the internet. They proposed that privacy could be broken down into discrete categories, such as informational privacy (Burgoon et al., 1989; Clarke, 1992). During this period, informational privacy began to attract significant academic attention. For instance, Burgoon et al. (1989) define informational privacy as "the ability to control who gathers and disseminates information about oneself or one's group, and under what circumstances." With the widespread adoption of the Internet, Clarke (1992) advanced the notion of privacy as personal data, aligning closely with informational privacy, especially regarding the collection, storage, and processing of data in digital contexts.

However, despite the increasing prominence of informational privacy, it did not immediately emerge as the dominant form of privacy. Instead, it coexisted with other forms, such as bodily, physical, and psychological privacy. This parallel structure persisted until Koops et al. (2017) introduced a new perspective, suggesting that privacy should be viewed as an overarching aspect of all other privacy types rather than a parallel or separate type. Notably, they believe that each of the other privacy types contains an element of information privacy - that is, a privacy may exist either in restricting access or controlling the use of information about each type of privacy (Koops et al., 2017). As an illustration of their argument, they make the reasonable

and logical case that behaviour privacy is not limited to restricting access to personal behaviours in public spaces, but also to controlling information about those same behaviours (Koops et al., 2016). This reasoning highlights that the core of informational privacy lies in controlling personal information control- that is the protection of who gathers and disseminates information about oneself and under what circumstances (Li, 2011; Smith et al., 1996; Westin, 1968).

2.3.2 Introduction of Smith et al.'s (2011) Information Privacy Conceptualisation

Building on a wealth of privacy studies, Smith et al. (2011) identified four main approaches academics conceptualise informational privacy. The first school of thought, "privacy as a right", holds that it is a person's right to decide when, how, and with whom information is shared. Warren and Brandeis's (1890) "right to be left alone" is the most representative definition. The second, "privacy as commodity" holds that privacy is not an absolute right but is subject to the economic principles of cost-benefit analysis, which states that consumers would use their personal information to exchange for benefits. This economic component of privacy has usually been used to explain individuals' self-surveillance phenomenon of voluntarily providing information online.

The third school of thought, "privacy as a state", holds that privacy could be characterised as "a person's state of limited access to infrastructural resources". The

representative definitions include Weinstein's (1971) definition of general privacy as a state of "being apart from others (p. 626)". The fourth school of thought, "privacy as control", holds that privacy is the ability of the individual to control the terms under which personal information is acquired and used. Margulis (1977) proposed a control-centred privacy definition: "Privacy, as a whole or in part, represents the control of transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or to minimize vulnerability (1977, p. 10)".

A later review of privacy definitions across key empirical studies in the context of online behavioural advertising (OBA) reveals a dominant trend: the majority of studies adopt definitions related to informational privacy. Notably, Westin's (1968) foundational notion that privacy is "the ability of the individual to control the terms under which personal information is acquired and used", is explicitly cited in numerous studies, such as those by Bleier and Eisenbeiss (2015) and Zarouali et al. (2017). Burgoon et al.'s (1989) definition, "the ability to control and limit physical, interactional, psychological, and informational access to the self or one's group" (p.132), is cited by studies including Baek and Morimoto (2012), Jung (2017), Kim and Huh (2017), and Nyheim et al. (2015). This trend demonstrates that Smith et al.'s (2011) conceptualisation of "privacy as control" remains the prevailing lens, even across diverse regulatory and cultural environments in the OBA context. Ultimately, the concept of information privacy in OBA revolves around personal information

control, specifically, determining who gathers and disseminates consumer information in the context of OBA (Li, 2011; Smith et al., 1996; Westin, 1968). (Li, 2011; Smith et al., 1996; Westin, 1968).

2.4 Privacy Measurements

Building on the previous review of privacy definitions, which revealed a strong conceptual emphasis on information privacy, particularly through the lens of "privacy as control", it is equally important to consider how these definitions are translated into empirical measurement (Stern et al., 2001). Specifically, this raises the question: do existing measurement tools align with the conceptual foundations of information privacy "as control", or is there a disconnect? To address this, the following section shifts focus to this empirical dimension by reviewing the primary privacy measurement scales used in OBA studies.

Table 1 summaries the privacy scales used by OBA studies. As shown in Table 1, the measurement scales of privacy are commonly framed as scales of privacy concerns. Although these scales are often designed to capture individuals' privacy concerns, they are used to operationalise consumer privacy, given that the construct of *privacy concerns* has long been used as a measurable proxy for individual privacy (Smith et al., 2011). When reviewing the scales summarised in Table 1, there is a lack of

measurement tools specifically designed for OBA contexts. Researchers have largely relied on adapted versions of earlier scales originally designed for information privacy concerns. For instance, several OBA studies adapt the prior scales (scales 1-4 in Table 1) (Brinson et al., 2019; Gironda & Korgaonkar, 2018; Ham, 2017; Jung, 2017; Kim & Huh, 2017; Mpinganjira & Maduku, 2019; Yang, 2013; Zarouali, 2017); while others directly use Baek and Morimoto's (2012) scale which is designed for online personalised advertising (Bol et al., 2018; Nyheim et al., 2015; Smit et al., 2014; Strycharz et al., 2019).

Among these scales, the most widely cited and used instrument in OBA is Baek and Morimoto's (2012) scale (Scale 5), which appears in numerous studies across the literature. However, it is important to note that this scale itself is an adaptation of Dolnicar and Jordaan's (2007) earlier instrument (Scale 4), originally developed for direct marketing. That scale aimed to measure consumers' concerns about potential intrusions and the unwanted disclosure of personal information. As such, foundationally, the measurement instruments most commonly used in OBA research trace back to Scales 1 through 4.

A close examination of these existing information privacy concern scales reveals a consistent dominance of the "privacy as control". Although the scales differ in dimensions and item phrasing, the underlying emphasis on individual control over

personal information remains clear and persistent. For example, the Smith et al.'s (1996) CFIP scale, incorporates dimensions such as "unauthorised secondary use", "improper access", and "collection", all of which implicitly or explicitly relate to individuals' loss of control over how their data is collected, shared, or used without consent. Items like "companies should not use personal information unless authorised" directly reflect this concern with control. Malhotra et al.'s (2004) IUIPC scale makes this link even more explicit by incorporating a dedicated "control" dimension, with items such as: "I believe I have the right to exercise control and autonomy over decisions about how my information is collected, used, and shared."

Subsequent models such as Dinev and Hart (2004), Dolnicar and Jordaan (2007), and Baek and Morimoto (2012) build upon these foundations by including items related to misuse, unauthorised disclosure, and lack of transparency. While they occasionally include dimensions such as "government protection," "privacy policies," or "solicitation" (as in Dolnicar and Jordaan's scale), these are typically evaluated through the perspective of how they enable or hinder consumer control. Across all these scales, a theoretical consistency emerges: privacy is conceptualised as control over personal information - specifically, control over who collects it, who uses it, and under what circumstances (Li, 2011; Smith et al., 1996; Westin, 1968).

Table 1. *Pre-existing information privacy concerns scales*

Studies	Number	Model's name	Dimensions of privacy concerns	Items
Smith et al. (1996)	Scale 1	Concerns of information privacy (CFIP)	"collection"	1. It usually bothers me when companies ask me for personal information. 2. When companies ask me for personal information, I sometimes think twice before providing it. 3. When people give personal information to a company for some reason, the company should never use the information for any other reason. 4. I'm concerned that companies are collecting too much personal information about me.
			"errors"	1. All the personal information in computer databases should be double-checked for accuracy-no matter how much this costs. 2. Companies should take more steps to make sure that the personal information in their files is accurate. 3. Companies should have better procedures to correct errors in personal information. 4. Companies should devote more time and effort to verifying the accuracy of the personal information in their databases.
			"Unauthorised secondary use"	1. Companies should not use personal information for any purpose unless it has been authorised by the individuals who provided the information. 2. When people give personal information to a company for some reason, the company should never use the information for any other reason. 3. Companies should never sell the personal information in their computer databases to other companies.
			"improper access"	1. Companies should devote more time and effort to preventing unauthorised access to personal information. 2. Computer databases that contain personal information should be protected from unauthorised access-no matter how much it costs. 3. Companies should take more steps to make sure that unauthorised people cannot access personal information in their computers.
	Scale 2		"control"	(1) Consumer online privacy is really a matter of

Malhotra et al. (2004)		Internet users' information privacy concerns (IUIPC)		consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared. (2) Consumer control of personal information lies at the heart of consumer privacy. (3) I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction.
			"collection"	(1) It usually bothers me when online companies ask me for personal information. (2) When online companies ask me for personal information, I sometimes think twice before providing it. (3) It bothers me to give personal information to so many online companies. (4) I'm concerned that online companies are collecting too much personal information about me.
			"awareness of privacy practices"	(1) Companies seeking information online should disclose the way the data are collected, processed, and used. (2) A good consumer online privacy policy should have a clear and conspicuous disclosure. (3) It is very important to me that I am aware and knowledgeable about how my personal information will be used.
Dinev and Hart (2004)	Scale 3	Internet individuals' privacy concerns	"abuse"	(1) I am concerned that the information I submit on the Internet could be misused. (2) When I shop online, I am concerned that the credit card information can be stolen while being transferred on the Internet. (3) I am concerned about submitting information on the Internet, because of what others might do with it. (4) I am concerned about submitting information on the Internet, because it could be used in a way I did not foresee.
			"findings"	(1) When I am online, I have the feeling of being watched. (2) When I am online, I have the feeling that all my clicks and actions are being tracked and monitored. (3) I am concerned that a person can find the following information about: • My date and place of birth, and the names of my parents,

				• Names and information about my immediate family members, • Addresses and telephones of my home/workplace, • Address and telephone of my current and Previous residences, • The location, the appraisal, and the price I paid for my assets/properties (house/apartment), as well as all the detailed information about my house, • My driving records, • Credit card/mortgage/other credit records
Dolnicar and Jordaan (2007)	Scale 4	Direct Marketing Consumer information privacy concerns (CIPC)	"data collection" "data storage and security" "data use" "data disclosure and dissemination" "solicitation" "privacy protection policies" "legislation and government protection" "behavioural intentions"	(1) I fear that personal information may not be safe while stored. (2) Information is safe while stored in a company's records. (3) I believe that companies use information for other purposes. (4) Consumer information is misused. (5) I am concerned about misuse. (6) I feel uncomfortable when companies share information. (7) Companies share information with others without permission. (8) Companies regularly share information with others to offer products. (9) Companies send too much advertising material. (10) Too many companies call to sell products and services. (11) I don't mind receiving telephone calls. (12) I receive too much advertising material. (13) Consumers not interested in getting information from unfamiliar companies. (14) Pleased to receive information from unfamiliar companies. (15) Companies must have privacy protection policies. (16) Companies should have privacy protection policies. (17) Companies should have privacy protection policies indicating reasons for protection.

				(18) Policies should indicate how they will protect information. (19) Government should restrict information collection. (20) Government should do more to protect safety of information. (21) Government should limit companies use of information. (22) I request company to remove information if misused. (23) I request removal of information if sold to others. (24) I would support a company's effort to ensure safety. (25) I refuse to provide personal information without a reason supplied.
Baek and Morimoto (2012)	Scale 5	Personalised advertising Consumer information privacy concerns (CIPC)	Not identified	When I receive personalised advertising on [MEDIA TYPE], 1. I feel uncomfortable when information is shared without permission. 2. I am concerned about misuse of personal information. 3. It bothers me to receive too much advertising material of no interest. 4. I feel fear that information may not be safe while stored. 5. I believe that personal information is often misused. 6. I think companies share information without permission.

2.5 Conclusion and Implications

This chapter offers an overview of definitions and measurements of consumer privacy, which are the two important aspects of privacy conceptualisation in the context of OBA. The review of consumer privacy definitions reveals a conceptual evolution from broad normative ideals to more context-specific formulations, with a

clear emphasis on information privacy as the dominant conceptualisation. Early legal definitions have been challenged by the complexities of digital technologies and consumer behaviour. This has led scholars to develop more nuanced types and definitions of privacy. With the widespread use of the Internet, information privacy, particularly in relation to control over the collection, use, and dissemination of personal data, has become central in contexts like OBA.

The review of consumer privacy measurements reveals a significant gap: there is no dedicated operational scale specifically developed for the unique privacy challenges posed by OBA. Instead, existing research predominantly adapts from earlier information privacy concern scales. The most frequently adopted is Baek and Morimoto's (2012) scale, which, despite being designed for personalised advertising, is itself adapted from earlier scales developed outside the OBA context. A deeper analysis of these scales reveals a strong theoretical coherence around the concept of privacy as control. Whether implicitly embedded in dimensions such as "unauthorised secondary use" and "improper access" (Smith et al., 1996) or explicitly operationalised through a dedicated "control" dimension (Malhotra et al., 2004), the notion that privacy concerns stem from a perceived loss of control over personal information remains consistent.

The strong alignment between definitions and measurements of information privacy in the context of OBA suggests a predominant reliance on the "privacy as control"

conceptualisation. However, this emphasis may overshadow alternative conceptualisations of privacy, such as privacy as a right or as a state, which are equally relevant to understanding consumer privacy in OBA. This pattern highlights the need for a more comprehensive and critical analysis of the full range of privacy conceptualisations. To address this gap, a later chapter will closely examine Smith et al.'s (2011) four-category privacy conceptualisation approaches. Through this examination, it seeks to uncover theoretical limitations within each category and identify the conceptualisation most aligned with a *critical scientific realism* (Niiniluoto, 1999) of consumer privacy.

Chapter 3: Empirical Privacy Research in OBA – Literature Overview

3.1 Introduction

To address the second notable issue raised in the background - namely, the consumer privacy empirical findings, this chapter provides an overview of empirical research examining consumer privacy concerns in the context of OBA. Rather than offering an exhaustive review, this chapter focuses on identifying key research strands associated with consumer privacy concerns in OBA, that is, the antecedents, outcomes, and interrelationships of consumer privacy concerns. Through mapping and conducting an inductive thematic analysis of these elements, the review seeks to characterise the fundamental nature of existing empirical findings, thereby laying a structured foundation for the critical evaluations to be undertaken in the subsequent chapters.

Notably, the area of the previous discussion focuses on the conceptualisation of privacy in OBA, whereas this chapter shifts its attention to the empirical research surrounding privacy concerns (not privacy *per se*) in OBA. While these two aspects might seem distinct sat first glance, they are closely interconnected. The construct of privacy concerns has long been used as a measurable proxy for consumer privacy (Smith et al., 2011). This means that privacy and privacy concerns are not mutually exclusive; they essentially represent the same underlying concept. As such, reviewing the empirical evidence on privacy concerns in OBA is justified in evaluating the accuracy and depth of consumer privacy conceptualisation.

3.2 The Necessity and Structuring of Reviewing Empirical Privacy Research in OBA

The growing proliferation of OBA has made consumer privacy a critical area of focus in academic and policy debates (Boerman et al., 2017; Zuboff, 2019). Given the rapid expansion of OBA practices, empirical studies have demonstrated that consumers' privacy concerns significantly influence their general attitudes toward OBA (Brinson et al., 2019; Kim & Huh, 2017), their overall trust in the brand (Mpinganjira & Maduku, 2019), and their acceptance or resistance to OBA (Boerman et al., 2017). However, discrepancies persist regarding the drivers of these concerns across different cultural, regional, and personal environments (Brinson & Eastin, 2016; Smit et al., 2014; Strycharz et al., 2019). Similar inconsistencies appear in studies examining the relationship between privacy concerns and click intentions (Bleier & Eisenbeiss, 2015; Kim & Huh, 2017).

As Krasnova et al. (2009) argued, inconsistent findings on privacy concerns in online social networks have hampered the development of cumulative knowledge of privacy concerns and behaviours. Similarly, fragmentation and inconsistency in consumer privacy research within OBA potentially impede the formation of a thorough and cohesive understanding of the field. Therefore, a systematic review of empirical research is essential to clarify the fragmented and often contradictory findings in the literature of consumer privacy concerns in OBA.

To ensure a structured review, consumer privacy concerns are positioned as the central construct, consistent with established privacy models in Chapter 6, such as Smith et al.'s (2011) Antecedents-Privacy Concerns-Outcomes (APCO) model and Li's (2011) Integrative framework on Concerns for Information Privacy (CFIP). These models have been instrumental in synthesising privacy research by placing privacy concerns as the central construct between antecedent stimuli and outcomes. Furthermore, both models highlight the mediating and moderating roles that privacy concerns may play in influencing other variables. Accordingly, empirical findings of consumer privacy concerns in OBA are systematically organised into three categories: (1) Antecedents of privacy concerns, (2) Outcomes of privacy concerns, (3) Interrelationships (mediations and moderations) involving privacy concerns. Table 2 provides an overview of how the current empirical findings are structured within this framework.

When looking at Table 2, it should be clarified that the groups of variables within each categorisation emerged inductively from thematic clustering of empirical findings during the review process. Specifically for antecedents, five key groups of stimuli were identified inductively through thematic analysis: Ad-controlled characteristics, demographic factors, consumer knowledge, cognitive appraisal processes, and personal factors. A similar thematic analysis was applied to the outcomes. As Lambert (2012) argued, the thematic analysis enables researchers to

break down a text into more manageable themes. These groupings aim to balance parsimony with comprehensiveness, ensuring that major empirical findings are captured while laying a manageable foundation for the critical appraisal undertaken in the following chapter.

Table 2. *Antecedents and outcomes of consumer privacy concerns in OBA: An inductive synthesis of empirical findings*

Inductive Groups	Proposed Relationships	Empirical Findings	Supporting studies	Inconsistent findings
Antecedents → Consumer Privacy Concerns				
Ad-Controlled Characteristics	Ad personalisation	Positive and Significant (context- and trust-dependent)	Bleier & Eisenbeiss (2015); Bol et al. (2018)	—
	OBA transparency (i.g, visual privacy protection methods)	Negative and Significant	Stanaland et al. (2011)	—
Demographics	gender, education, income	Females, lower education and income report higher concerns	Smit et al. (2014); Hoy & Milne (2010); Awad & Krishnan (2006)	—
Consumer knowledge	Consumer knowledge of OBA	Positive and Significant	Ham (2017); Wohn et al. (2015)	No effects in European (Brinson & Eastin, 2016; Smit et al., 2014; Strycharz et al., 2019)
Cognitive Appraisal Process	Threat appraisal variables			
	Perceived risks	Positive and Significant	Ham (2017)	—
	Perceived benefits	Positive and Significant	Jung (2017); Palos-Sanchez et al., (2019)	Negative and Significant (Ham, 2017)
	Coping appraisal variables			
	Perceived privacy control	Negative and Significant	Gironda & Korgaonkar (2018); Mpinganjira & Maduku (2019)	—
	Self-efficacy	Positive and Significant	Ham (2017)	No significant relationship (Wohn et al., 2015)
Consumer Personal Factors	Desire for privacy	Positive and Significant	Gironda & Korgaonkar (2018); Mpinganjira & Maduku (2019); Stanaland et al. (2011)	—
	Past negative experience	Positive and Significant	Yang (2013)	—

Consumer Privacy Concerns → Outcomes				
Attitudes	General attitudes toward OBA	Negative and Significant	Brinson et al. (2019); Kim & Huh (2017);	—
Perceptions	Ad scepticism	Positive and Significant	Baek & Morimoto (2012); Zarouali et al. (2017)	—
	Perceived intrusiveness	Positive and Significant	Gironda & Korgaonkar (2018); Mpinganjira & Maduku (2019); Van Doorn & Hoekstra (2013)	—
	Perceived risks	Positive and Significant	Yang (2013)	—
	Trust in advertisers	Negative and Significant	Brinson et al. (2019)	—
Behaviour	Opt-out	Non-significant	Strycharz et al. (2019)	—
	Self-disclosure behaviour	Non-significant	Bol et al. (2018)	—
	Purchase intention	Negative and Significant	Van Doorn & Hoekstra (2013)	—
	Ad avoidance	Positive and Significant	Ham (2017); Baek & Morimoto (2012); Jung (2017); Nyheim et al. (2015)	—
	Click behaviour	Negative and Significant	Bleier & Eisenbeiss (2015)	No significant effect (Kim & Huh, 2017; Gironda & Korgaonkar, 2018)
Interrelationships – Mediation vs. Moderation				
Privacy concerns as mediator	Mediates effects between perceived risk and ad avoidance	Significant	Ham (2017)	—
	Mediates effects between self-efficacy and ad avoidance	Significant	Ham (2017)	—
	Mediates effects between desire for privacy and perceived invasiveness	Significant	Gironda & Korgaonkar (2018)	—
	Mediates effects between perceived control and perceived invasiveness	Significant	Gironda & Korgaonkar (2018)	—
Privacy concerns as moderator	Moderates perceived personalisation and ad engagement	Significant	Noor et al. (2019)	
	Moderates indirect effects between retargeting and purchase intention via ad scepticism	Significant	Zarouali et al. (2017)	

Source: Authors' Compilation.

3.3 Selections of Empirical Research of Consumer Privacy in OBA

Following the methodology recommended by Smith et al. (2011) for selecting empirical literature, a comprehensive review of research on consumer privacy in online behavioural advertising (OBA) was conducted. An initial pool of relevant studies was compiled by consulting prior OBA literature reviews by Varnali (2021) and Boerman et al. (2017). To capture recent developments in the field, this pool was supplemented with a Google Scholar (GS) search for studies published after 2020.

In selecting sources, particular attention was paid to the breadth and quality of databases. Scopus was employed to ensure the inclusion of high-quality sources, given its extensive indexing of academic publications (Meho & Yang, 2007). GS was additionally used to capture broader materials, despite its relatively lower quality control (Meho & Yang, 2007). The following keywords guided the search process: “online behavioural advertising,” “online personalised advertising”, “OBA”, “privacy concerns”, and “privacy”. This search strategy resulted in an initial sample of 167 articles.

To refine the sample and focus specifically on empirical research, the classification criteria outlined by Smith et al. (2011) were applied to distinguish *normative* from *descriptive* studies. Legal studies on OBA were categorised as normative and

excluded from this review. In contrast, literature employing qualitative or quantitative empirical methods was classified as descriptive and retained. Through this refinement process, a final set of 99 empirical studies was identified for analysis.

3.4 Antecedents of Privacy Concerns

As outlined in Section 3.2, this chapter organises empirical research around three major areas: antecedents, outcomes, and interrelationships involving privacy concerns. This section provides an overview of the first area, focusing on the antecedents of consumer privacy concerns in OBA. Drawing on an inductive thematic analysis of 99 empirical studies, five major groups of antecedents have been identified: ad-controlled characteristics, demographic factors, consumer knowledge, cognitive appraisal processes, and consumer personal factors. Each group reflects distinct but interconnected influences on how consumers perceive privacy risks in the context of OBA. The following subsections summarise empirical findings related to each group, noting variations across studies where relevant.

3.4.1 Ad-Controlled Characteristics

According to Boerman et al. (2017), ad characteristics (of OBA) is the first dimension of ad-controlled characteristics. Ad characteristics has two sub-dimensions: level of personalisation and OBA accuracy. The first sub-dimension, ad personalisation, whose predictive role of consumer privacy concerns in OBA has been supported. A

lab experiment conducted by Bleier and Eisenbeiss (2015), using a sample of 252 college students supports the hypothesis that various combinations of ad personalisation degrees are linked to consumer privacy concerns under the influence of trust in the retailer. There were three different OBA materials created using the depth vs. breadth dimensions of ad personalisation: (1) OBA combining high depth and narrow breadth featured either one of the three cameras on participant's wish list; (2) OBA combining high depth and wide breadth featured all three cameras on participant's wish list; (3) the banner with the retailer's logo only is low depth. According to the findings, OBA (1) does not raise privacy concerns among more trusted retailers; however, for less trusted retailers, both OBA (1) and (2) trigger privacy concerns. Interestingly, the moderator effect of retailer trust ceased to exist in OBA (2), which has the highest level of personalisation. That is, OBA (2) tends to raise consumer privacy concerns in both less and greater trust retailers.

Bol and colleagues (2018) further found that the effects of perceived personalisation on consumer privacy concerns differed slightly between the contexts of news, commerce, and health. Specifically, higher levels of perceived personalisation were associated with increased privacy concerns in the news and commerce contexts, whereas no significant effect was observed in the health context. Although the overall differences across contexts were relatively modest, these findings suggest that the relationship between perceived personalisation and privacy concerns may vary

depending on the type of online environment/situation in which OBA appears (Bol et al., 2018).

The second dimension of ad-controlled characteristics, as categorised by Boerman et al. (2017), is OBA transparency, which includes privacy statements and informed consent requests and disclosure methods. Notable research has shown that the presence (versus absence) of privacy trust marks, visual seal icons placed on OBA indicating adherence to high ethical standards, significantly influences consumer privacy concerns (Stanaland et al., 2011). Specifically, Stanaland et al. (2011) found that the effect of privacy trust marks was moderated by consumers' prior attitudes towards advertising and their desire for privacy. When people's desire for privacy was strong, having the privacy trust mark (as opposed to not having it) led to fewer privacy concerns. The effects ceased to exist when people's desire for privacy were low. In addition, a privacy trust mark had no effect on consumer privacy concerns when prior attitudes toward advertising were positive.

3.4.2 Demographic Factors

In existing research on privacy concerns in online behavioural advertising (OBA), relatively limited attention has been given to the demographic differences in consumer privacy concerns. Based on the literature review conducted for this chapter, only Smit et al. (2014) offer a detailed empirical investigation into how demographic variables such as gender, educational background, and income relate to consumer

privacy concerns within the context of OBA. Drawing on an analysis of 2,022 European participants, their study found that consumers who expressed a high level of privacy concerns were more likely to be female, have lower educational backgrounds, and come from lower income families. They had a more negative view of OBA, and were more concerned with safeguarding their personal information than the other groups (Smit et al., 2014). In contrast, consumers with lower level of privacy concerns were predominantly men with higher education levels, greater knowledge of cookies and OBA, and slightly higher incomes.

Although relatively few studies have prioritised demographic factors as primary predictors of privacy concerns, their influence should not be overlooked. For example, gender differences have been found to significantly predict young adults' privacy concerns on Facebook (Hoy & Milne, 2010), while both gender and age differences have been linked to online users' privacy concerns in the context of online personalisation (Awad & Krishnan, 2006). Although these studies were conducted outside the specific context of OBA, they remain highly relevant: Facebook is one of the key social media platforms where OBA has been targeted at consumers (Zarouali et al., 2017), and personalisation is the core mechanism underlying OBA, largely deciding its effectiveness (Aguirre et al., 2015; Boerman et al., 2017). These findings, therefore, serve as important points of reference for research on privacy concerns in OBA. Given that demographic factors have been recognised as influential predictors of privacy concerns, they warrant careful consideration in the context of OBA.

Accordingly, demographic variables have been included as a set of antecedents of consumer privacy concerns within this PhD project.

3.4.3 Consumer Knowledge

Consumer knowledge mainly relates to consumers' understanding of how to protect their privacy and their understanding of OBA, including its functioning mechanisms and aims. However, as can be clearly observed from Table 2, empirical research in OBA literature has produced inconsistent findings regarding the influence of consumer knowledge on privacy concerns. For example, using a sample of 544 US college students and 179 US internet users, respectively, both Ham (2017) and Wohn et al. (2015) confirmed that OBA knowledge directly and positively predicts US privacy concerns. By contrast, knowledge of OBA barely impacts the privacy concerns of European consumers (Brinson & Eastin, 2016; Smit et al., 2014; Strycharz et al., 2019). This inconsistent result regarding the effect of consumer knowledge on their privacy concerns in OBA may imply that cultural norms may moderate the predictive effect of consumer knowledge on consumer privacy concerns.

3.4.4 Cognitive Appraisal Process

People's cognitive appraisal process is commonly conceptualised in terms of t*hreat appraisal* and *coping appraisal*, concepts derived from Protection Motivation Theory, originally developed by Rogers (1975, 1983). The theory was proposed to explain how individuals respond to perceived threats and how such perceptions motivate

protective behaviours. Within this theory, the *threat appraisal* involves their weighing the perceived risks and benefits of persuasion tactics, while the *coping appraisal* relates to their ability to implement coping responses.

In the context of OBA, variables related to *threat appraisal* in terms of perceived severity and perceived reward have been studied as predictors of consumer privacy concerns. Those capturing consumers' perceptions of privacy severity have been examined as predictors of privacy concerns. For example, consumers' perceived risks regarding conscious and unintentional privacy breaches, data misuse, unauthorised data sharing, and other unanticipated issues have been shown to positively influence consumer privacy concerns (Ham, 2017).

In addition to risk-related variables, those capturing consumers' perceptions of the potential rewards associated with OBA have also been examined, but with inconsistent findings. According to their definition, variables such as perceived benefits (Ham, 2017), perceived usefulness (Wohn et al., 2015), and perceived relevance (Jung, 2017; Palos-Sanchez et al., 2019) have been used to assess consumers' perception of OBA benefits. These variables consistently define whether OBA is directly related to the interests, needs, and values of consumers, as well as whether it can be used to provide better savings, products, and Internet services. However, as shown in Table 2, research revealed inconsistent results regarding the effects of perceived benefits on privacy concerns. Some studies report a negative and

significant relationship between perceived benefits and a reduction in privacy concerns (Ham, 2017), while others have found that the perceived usefulness of a product increases privacy concerns (Jung, 2017; Palos-Sanchez et al., 2019).

When reviewing *coping appraisal* in OBA, both variables of self-efficacy and perceived privacy (behavioural) control have been used to assess consumers' ability to protect their private information (Gironda & Korgaonkar, 2018; Ham, 2017; Mpinganjira & Maduku, 2019; Wohn et al., 2015). Regarding perceptions of privacy control, studies consistently reported that consumers who felt more confident about their ability to manage OBA privacy controls expressed fewer privacy concerns (Gironda & Korgaonkar, 2018; Mpinganjira & Maduku, 2019). However, as illustrated in Table 2, the findings of the effect of self-efficacy are inconsistent. For example, Ham (2017) found that consumers who had a high level of self-efficacy in OBA were more likely to have higher levels of privacy concerns. However, Wohn et al. (2015) found no statistical relationship between self-efficacy and consumer privacy concerns.

3.4.5 Consumer Personal Factors

In addition to the antecedents discussed above, several other variables have been found to significantly predict consumer privacy concerns in OBA, yet do not neatly fit within the previously identified groups. For example, research has shown that

teenagers' past negative experiences with sharing personal information online increase their privacy concerns (Yang, 2013). Research also found that consumer's desire for privacy (or disposition to value privacy) that reflect their overall inclination to preserve their privacy has been consistently serving as a positive predictor of privacy concerns (Gironda & Korgaonkar, 2018; Mpinganjira & Maduku, 2019; Stanaland et al., 2011).

Phelan et al. (2016) found through interviews that trust, social presence, and marginal risk each influence privacy concerns in distinct ways, depending on whether the privacy concern is intuitive or considered. Trust, for example, exerted a strong effect on both intuitive privacy concerns (a "gut feeling") and considered privacy concerns (a deliberate assessment of risks and benefits). In contrast, social presence, the feeling of being watched or monitored by data collectors and advertisers, primarily shaped intuitive privacy concerns and was less frequently cited as influencing considered concerns. Marginal risk, defined as the perceived threat of a new privacy intrusion, was rarely discussed as a factor influencing intuitive concerns, but was more commonly seen as affecting considered privacy concerns (Phelan et al., 2016).

Looking across the definitions of these variables, a coherent theme emerges: these variables largely originate from consumers' internal characteristics, perceptions, or previous experiences. Therefore, they are inductively grouped under the broader label

of consumer personal factors, which are recognised as antecedents shaping privacy concerns in the context of OBA. A comparison with the antecedents identified in Smith et al.'s (2011) Antecedents-Privacy Concerns-Outcomes (APCO) model and Li's (2011) Integrative framework on Concerns for Information Privacy (CFIP) further supports this classification. The groups of privacy experiences, personality differences, and individual factors in these models similarly reflect the predictive role of personal factors.

3.5 Outcomes of Privacy Concerns

Following the overview of antecedents, this section addresses the outcomes associated with consumer privacy concerns in the context of OBA. Consumer privacy concerns have been found to influence a range of consumer responses. By organising these outcomes into three main categories, attitudes, perceptions, and behaviours, this section provides a structured overview of how privacy concerns shape consumer responses with OBA, while noting variations observed across different studies.

3.5.1 Attitudes

One of the most consistently examined outcomes of privacy concerns in OBA research is consumers' general attitudes toward OBA. Consumers' privacy concerns are a predictor of their general attitudes toward OBA (Brinson et al., 2019; Kim &

Huh, 2017; Mpinganjira & Maduku, 2019). Specifically, the more people are concerned about their privacy, the more negatively they attitudinally respond to OBA (Brinson et al., 2019; Kim & Huh, 2017).

Some studies also found that these negative attitudes toward OBA further shape perceptions of a brand's ethical value (Mpinganjira & Maduku, 2019), their clicking intentions (Kim & Huh, 2017), , and ad avoidance behaviour (Baek & Morimoto, 2012).

These findings suggest that attitudes toward OBA function as an important outcome of privacy concerns, and may serve as an intermediate mechanism through which privacy concerns shape subsequent consumer responses to OBA. Examining attitudes is, therefore, important for understanding how privacy concerns translate into broader consumer perceptions and behavioural tendencies in the OBA context.

3.5.2 Perceptions

Consumer privacy concerns critically shape a range of consumer perceptions, including ad scepticism (Baek & Morimoto, 2012; Zarouali et al., 2017), perceived trustworthiness to advertisers (Brinson et al., 2019), perceived intrusiveness (Gironda & Korgaonkar, 2018; Mpinganjira & Maduku, 2019; Van Doorn & Hoekstra, 2013),

and perceived risks (Yang, 2013). Ad scepticism, which is the tendency to disbelieve the informational claims in advertising (Obermiller et al., 2005), is higher among consumers with greater privacy concerns (Baek & Morimoto, 2012; Zarouali et al., 2017). It has also been reported that when consumers' privacy concerns grew, their trust in advertisers began to diminish (Brinson et al., 2019).

A consistent pattern has emerged across countries, including Germany, the US, and South Africa: consumers with stronger privacy concerns report higher perceptions of intrusiveness, characterising OBA as invasive, disruptive, and intrusive (Gironda & Korgaonkar, 2018; Mpinganjira & Maduku, 2019; Van Doorn & Hoekstra, 2013). In addition, Yang (2013) confirmed that American teens' privacy concerns strongly predict their perceived risks. Together, these findings suggest that privacy concerns systematically and consistently heighten consumers' perceptions of the negative attributes of OBA experiences.

3.5.3 Behaviour

Although privacy concerns have not been found to be significantly influence opt-out behaviour (Strycharz et al., 2019) or self-disclosure behaviour (Bol et al., 2018), they have been found to influence other important behavioural responses related to ad effectiveness, such as purchase intentions and ad avoidance.

Consumers with higher privacy concerns are generally less willing to purchase products featured in ads (Van Doorn & Hoekstra, 2013). Furthermore, with higher privacy concerns, consumers are likely to engage in ad avoidance behaviour, which refers to "all actions by media users that differentially reduce their exposure to ad content" (Speck & Elliott, 1997). Ham (2017) found that consumers with higher privacy concerns intentionally ignored and disliked OBA, with these avoidance behaviours increasing alongside privacy concerns. These findings are echoed by Baek and Morimoto (2012), Jung (2017), and Nyheim et al. (2015).

As apparently shown in Table 2, the impact of privacy concerns on click behaviour, however, appears less consistent. While some studies found that privacy concerns negatively affect consumers' willingness to click on or engage with an advertisement (Bleier & Eisenbeiss, 2015), others, such as Kim and Huh (2017), found no significant effect after controlling for variables such as demographics, exposure frequency, time spent online, online product search frequency, attitude toward personalised advertising, and internet competency). Gironda and Korgaonkar (2018) reported no significant correlation between privacy concerns and click intentions. These discrepancies highlight that the behavioural outcomes of privacy concerns in OBA may vary depending on the type of engagement behaviour examined.

Research also found that consumer behaviours often stem from above attitudes and perceptions. For example, consumers' attitudes towards OBA have been shown to have a negative effect on ad avoidance behaviour (Baek & Morimoto, 2012). And heightened perceptions of intrusiveness has been found to reduce purchase intentions (Van Doorn & Hoekstra, 2013). These layered relationships suggest that consumer behaviour should be conceptualised as the final stage in the response process of privacy concerns with the context of OBA, which is potentially mediated by both cognitive perceptions and attitudinal responses to OBA.

3.6 Moderation and Mediation Effects of Privacy Concerns

The final area of focus identified in this section concerns the interrelationships involving privacy concerns, specifically their mediating and moderating roles within the OBA framework. Mediation occurs when privacy concerns transmit the influence of antecedent variables onto outcomes (Muller et al., 2005), while moderation refers to privacy concerns altering the strength or direction of these relationships (Muller et al., 2005). This section summarises empirical findings regarding the mediating and moderating functions of privacy concerns, highlighting how these roles have been observed across different studies.

Empirical evidence shows that, in some contexts, consumer privacy concerns act as a mediator. For instance, Ham (2017) found significant indirect effects of privacy concerns between perceived risk and ad avoidance, as well as between self-efficacy and ad avoidance. Similarly, Gironda and Korgaonkar (2018) reported mediation effects between a disposition to value privacy and perceived invasiveness, and between perceived privacy control and perceived invasiveness. These studies conceptualise privacy concerns as internal psychological mechanisms that channel the effects of consumer cognitive appraisal into perceptions or behavioural outcomes.

However, other studies position privacy concerns as a moderator. In Noor et al. (2019) research, they found that as privacy concerns increase, the relationship between perceived personalisation and online advertising engagement becomes stronger. Consumers with low privacy concerns react negatively to higher personalisation, while those with high privacy concerns show the opposite pattern. Similarly, Zarouali et al. (2017) found that privacy concerns, along with text debriefing, significantly moderated the indirect relationship between retargeting and purchase intention through ad scepticism, with stronger effects observed among adolescents with higher privacy concerns.

These findings further reveal a fragmented picture: some studies observe privacy concerns as mediating internal processes, while others see them as contextual moderators of external relationships. Moreover, even within similar theoretical

frameworks, the direction of these effects varies. This inconsistency highlights a broader conceptual ambiguity in the field, complicating efforts to build a unified understanding of how privacy concerns function within the OBA environment.

3.7 Discussion and Conclusion

This chapter offers an overview of empirical research on consumer privacy within the context of OBA, synthesising key factors associated with consumer privacy concerns, focusing on their antecedents, outcomes, and interrelationships among these elements.

While the existing body of research offers valuable empirical insights, the review reveals that findings remain fragmented. This fragmentation has been reflected at multiple analytical levels. First, fragmentation is evident in the dispersion of variables examined as antecedents and outcomes of privacy concerns. A wide array of antecedents has been identified, ranging from ad-controlled characteristics and demographic variables to consumer knowledge, cognitive appraisal processes, and personal factors. These antecedents originate from heterogeneous theoretical domains, including external stimuli, social-structural variables, cognitive evaluations, and personality-based traits. However, the literature does not provide a unified theoretical foundation that systematically integrates these influences, nor does it clearly distinguish between external stimuli and the internal organism of privacy concerns.

Privacy concerns are frequently treated as a conceptual “black box” into which diverse predictors are inserted without sufficient theoretical differentiation.

In addition, the same construct is often operationalised using different variables across studies. For example, variables such as perceived benefits (Ham, 2017), perceived usefulness (Wohn et al., 2015), and perceived relevance (Jung, 2017; Palos-Sanchez et al., 2019) have been used to assess consumers’ perception of OBA benefits.

Furthermore, the fragmentation is also reflected by the issue that the same construct is assigned different theoretical roles. For example, perceived risk is treated in some studies as an outcome of privacy concerns, while in others it functions as an antecedent as part of mediation pathways. Similarly, privacy concerns themselves are alternately conceptualised as mediators and moderators within different theoretical frameworks. Some studies conceptualise privacy concerns as mediating internal cognitive processes that link antecedents to behavioural outcomes, while others treat privacy concerns as contextual moderators that condition the relationship between external factors and consumer responses. This instability in conceptual positioning indicates a lack of clarity regarding the functional role of privacy concerns within OBA research.

Beyond this broader fragmentation, inconsistency is also evident at the level of specific empirical relationships. In many cases, findings regarding both antecedents and outcomes of privacy concerns remain inconsistent across studies. For example, while some studies (particularly within U.S. contexts) demonstrate that consumer knowledge positively influences privacy concerns, other research (especially in European contexts) fails to establish this effect. Inconsistencies are evident in whether self-efficacy significantly shapes consumer privacy concerns.

These inconsistencies extend to the consequences of privacy concerns. While many studies agree that privacy concerns significantly shape negative attitudes towards OBA and perceptions, the degree to which these concerns translate into behaviours is far less clear. For instance, consumer privacy concerns have been found to have little relevance in predicting behaviours such as opting out of OBA or self-disclosure. However, research found that privacy concerns significantly predict consumers' click-through rates, despite yielding contrasting results. For example, some studies report a significant link between privacy concerns and click intentions, whereas others find no such correlation. This conflicting evidence raises questions about the cognitive success of existing theoretical frameworks and further complicates efforts to clarify the behavioural outcomes associated with privacy concerns.

3.8 Implications

The preceding review reveals fragmented antecedents and outcomes of consumer privacy concerns, as well as inconsistent findings, particularly in relation to contextual variables, OBA knowledge, cognitive appraisal processes, and behavioural outcomes associated with privacy concerns. These patterns point to a critical need for a more in-depth analysis to uncover the underlying causes of such fragmentation and inconsistency.

To address this need, in Chapter 5, a deep and critical examination of these inconsistencies through the lens of established privacy theories will be undertaken. In doing so, it aims to identify potential theoretical limitations and conceptual ambiguities contributing to the fragmented nature and confounding findings of the existing research. Ultimately, this critical analysis, together with this review, will seek to offer a clearer and more coherent understanding of consumer privacy concerns in OBA, helping to establish a strong theoretical foundation for possible solutions to advance the field.

Chapter 4: Reconceptualising Privacy as a State – Critical Appraisal

4.1 Introduction

This chapter begins by exploring conceptual issues. Among all the conceptual problems, the issue of definition is the most critical. The thesis title suggests that to examine the impact of consumer privacy accurately, it is essential first to define it. Therefore, defining privacy is crucial. This section explores definitions of privacy in the context of online behavioural advertising (OBA). This chapter highlights key conceptual issues related to privacy by reviewing and critically analysing definitions and measurements of privacy. It critically evaluates Smith et al.'s (2011) four information privacy conceptualisation approaches. A scale analysis component is also incorporated, guided by a related research question, to assess whether existing measurement approaches are definition-driven: that is, which conceptualisations they capture and how adequately they assess them. It then argues for a transition from defining privacy as control to a state within the privacy field, and initially makes a case for this transition in OBA.

4.2 Critical Review of Smith et al.'s (2011) Information Privacy Conceptualisation

As introduced in the earlier chapter, Smith et al. (2011) offer one of the most influential frameworks for understanding information privacy, categorising four

distinct conceptual approaches used by prior privacy literature: privacy as a right, a commodity, a state, and control. This typology has become a key reference point in privacy scholarship, valued for its ability to bring clear structure to conceptualise privacy. By boiling diverse privacy definitions into four overarching categories, Smith et al. (2011) provide a useful foundation for researchers seeking to navigate how privacy has been conceptualised.

Yet, while this framework's significant value in synthesising and organising diverse conceptual approaches, as the following critical analysis will show, some of the dimensions, especially their conceptual foundations, appear to fall outside the theoretical and empirical remit of privacy research. As such, this section revisits each of the four dimensions, not simply to restate them, but to critically evaluate which conceptual approaches are more relevant to contemporary privacy research.

4.2.1 Privacy as a Right

A very early and ubiquitous definition of privacy describes it as a "right to be left alone" (Westin, 1968). Up to this point, privacy has been criticised as a catch-all term subsumed under the rubric of ethics and the society's moral value system (Smith et al., 2011). By contrast, whilst privacy as a right has become ubiquitous in the literature (Smith et al., 2011), this dimension does nothing to determine what privacy

is, in the same way as free speech as a right does not define free speech. For example, a widely cited example is that "privacy is the right to be left alone" (Westin, 1968) which would mean that the object of the right is "be left alone", which does not describe privacy but a variety of situations. Instead of trying to define privacy as a right, the best way to approach the rights question is to first define what privacy is before arguing whether this is something people should have a right to i.e., privacy must have a definition independent of whether it is a right. It is then possible to consider whether privacy should be a right.

4.2.2 Privacy as a Commodity

Similarly, if examining privacy as a commodity, the real point at issue is also what the commodity actually *is*. Although some libertarian political scientists argue that "privacy as a commodity" serves to explain the phenomenon of individuals voluntarily providing information online in exchange for perceived benefits (Smith et al., 2011), they do not explicitly clarify what the commodity is.

Another issue under this conceptualisation framework stems from the economic principles of "privacy as a commodity". From this principle, privacy is subject to the economic principles of cost-benefit analysis and trade-off. However, this is problematic. In describing privacy as a commodity, the implication points to it being a

tradeable good (e.g., Smith et al., 2011). Viewing privacy as a tradeable good is metaphorical. While metaphors, as Cornelissen (2003) notes, can aid in theory development, they are not literally accurate. This raises the question of whether viewing privacy as a tradeable good contributes meaningfully to the theory, which seems doubtful, given the lack of clarity about what exactly the "good" being traded is.

4.2.3 Privacy as Control

The notion of "privacy as control" has been widely accessed in the digital age (Bélanger & Crossler, 2011), especially in the field of information systems (Li, 2011) and marketing (Martin & Murphy, 2017). Following Burgoon et al. (1989)'s privacy definition, a thread of privacy research defines information people's privacy as their ability to control and limit informational access to themselves (Baek & Morimoto, 2012; Jung, 2017; Kim & Huh, 2017). Another thread of privacy research, following Westin's (1968) privacy definition, defines people's privacy as their ability to control the terms under which personal information is acquired and used (Bleier & Eisenbeiss, 2015; Zarouali et al., 2017). Thus, the control-based conceptualisation of privacy has at the core concept of personal information control- that it is about who gathers and disseminates information about oneself and under what circumstances (Li, 2011; Smith et al., 1996; Westin, 1968).

However, the approach of conceptualising privacy as control becomes particularly theoretically problematic in the digital age. “Privacy as control” presupposes that people have the “ability” to control transactions between persons and others (Smith et al., 2011). Nevertheless, this assumption becomes increasingly theoretically impractical in the digital age. Online tracking technologies have facilitated widespread data collection and surveillance, leaving online users with little to no control over their privacy (Büchi et al., 2022; Strycharz & Segijn, 2022). The key argument here is that before assessing how individuals control their information, it is essential to first determine whether they have any control over it. If the case is that consumers cannot possess efficient control over their personal information, the notion of “privacy as control” is theoretically tenuous, as consumers can only control their privacy in practice when true control is established.

Furthermore, as Hull (2015) argues, privacy as control relies too much on an economic perspective, causing its theoretical flaw. From an economic standpoint, “privacy as control” is associated with privacy self-management, which assumes that individuals are rational managers who behave rationally when expressing privacy preferences and that their actions accurately reflect these preferences. However, Hull (2015) contends that individuals cannot clearly express privacy preferences or accurately reveal them through behaviour due to information deficits and asymmetries between them and data-collecting entities, substantial required effort, and their social

constraints when expressing privacy preferences. By contrast, “privacy as control” promotes neoliberal governance, causing individuals to believe they are primarily responsible for poorly managed privacy risks (Hull, 2015). “Privacy as control” is a measurable result of a paradigm of scholarly shift, neglecting its utility from individual shift (Hull, 2015; Smith et al., 2011). Therefore, this perspective overemphasises economic choices in privacy management, focusing on privacy’s economic value while neglecting its social significance (Hull, 2015).

4.2.4 Privacy as a State

Of all Smith et al.’s dimensions, one of the least discussed but most important dimensions is the notion of “privacy as a state”. Weinstein (1971, p. 626) conceptualised general privacy as a state of “being apart from others,” articulated through four distinct substates: anonymity, solitude, reserve, and intimacy. Schoeman (1984, p. 3) defined general privacy as “a state of limited access to a person.” Due to the purpose of addressing information-based issues, this sought-after *state of limited access* was subsequently translated into *a state of limited access to information* (Smith et al., 2011).

This is important as it would be difficult to argue that privacy is not a heterophenomenological state of mind for people, which Dennett (2007, p. 249)

describes as “a level of first-person description of the conscious dimension of cognitive properties, corresponding to the phenomenological properties of cognition”. This is important as it would be difficult to argue that privacy is not a heterophenomenological phenomenon, but an experience where an individual can describe their perception of a privacy state in a given context. If asking a person if they have a sense of privacy in a given context, they will understand this question and will answer the question based on their state of mind in that context. For example, Laufer and Wolfe (1977) found that even children are capable of articulating their privacy experiences across three dimensions (i.e. self-ego, environmental, and interpersonal) by expressing the emotional states associated with those experiences.

> With respect to the self-ego dimension, Laufer and Wolfe (1977) argued, “Children in explaining why situations they described as private were experienced as private give reasons connected with autonomy: “I felt independent,” “I could do what I wanted to do,” “I could have my own opinions.” (p. 27)”

> Regarding the environmental dimension, they supported the concept of privacy as a state by finding that “one of the only places for privacy as physical aloneness was an uncomfortable seclusion room where children were sent when they “acted

out." Nevertheless, because it permitted solitariness, some children said they feigned emotional upset to have access to the room (p. 29)."

In interpersonal situations, they also found privacy states as follows: "the most significant point about these invasion experiences was that intruders were most often siblings, that is, were of like status within the family system. Our respondents reported anger at invasion; they used such terms as "awful," "hurt," "afraid," "very upset." (p. 35)"

Therefore, individuals express their privacy experiences by conveying self-described conscious feelings (either genuine or feigned), such as "feeling independent," "upset," and "awful". This supports the argument that privacy is a heterophenomenological state of mind for people.

4.3 Privacy as a State: A New Privacy Definition

Viewing privacy as a state has clear benefits, particularly in providing a coherent definition of privacy (see below). When presenting the definition of privacy as a state, it is important to emphasise the relationship between individuals' perception of control and privacy as a state. As Koops et al. (2016) contend that "privacy may exist either in restricting access or controlling the use of information about each type of

privacy (p. 569)". The impact of control on privacy state suggests that control, while not privacy *per se*, is essential in leading to a state of privacy.

This perspective is also embedded in other theories. For example, Laufer and Wolfe (1977) argue that control over personal (or sometimes group) information is the foundation of the heterophenomenological experience of privacy, where the disclosure of personal information can alter the state. Similarly, Petronio's (2020) communication privacy management theory suggests that a breakdown in information control results in a state of "privacy turbulence (2020, p. 77)". Together, these perspectives confirm the argument that individuals' perception of control over sensitive personal/group information is a factor that shapes people's privacy state. Therefore, this argument has been highlighted in my definition of privacy.

Based on the above considerations, I present a new definition of privacy premised on the idea of privacy as a state as follows:

Privacy is a state of mind, as perceived by an individual or a state of mind of members of a group, whereby the state of mind is determined by a perception of the degree of control over sensitive personal/group information that third parties can access. States of privacy sit on a continuum between no privacy and complete privacy.

Given this definition, there are three possible states which can be applied in a particular context: (1) I have privacy in this context, (2) I have partial privacy in this context, and (3) I have no privacy in this context (Smith et al., 2011). In this definition, the perception of the degree of control over sensitive personal/group information is essential to set boundaries around the privacy concept by specifying that privacy must be about the control of sensitive information accessible to third parties (Morse et al., 1996).

My definition is further supported by Smith et al. (2011), who suggest that "there must be a continuum of states of privacy from absolute to minimal (p. 995)". Acquisti et al. (2015) similarly argue that "individuals can, depending on the situation, exhibit anything ranging from extreme concern to apathy about privacy (p. 511)". Consequently, I also take into account the dynamic range of privacy states in the new definition of privacy.

This definition highlights the social value of privacy, a dimension largely overlooked in the "privacy as control" conceptualisation. As examined in the earlier section on "privacy as control", the overemphasis on economic values leads to its neglect of privacy's social value (Hull, 2015). However, defining "privacy as a state" highlights

its social value, providing a framework for understanding privacy from a social perspective. Following Hull's (2015) argument, this thesis argues that the conceptualisation of "privacy as a state" inherently underscores privacy's social value, from how privacy contributes to individual flourishing to how it influences the ways people engage in social networks.

According to Hull (2015), privacy plays a crucial role in maintaining social structures that enable individuals to flourish: "Privacy is essential to the maintenance of the social networks within which individuals can flourish (Hull, 2015, p. 94)". As noted from Laufer and Wolfe (1977), individuals interact with their social environments by perceiving both phenomenological and normative aspects of privacy from self-ego, environmental, and interpersonal perspectives. This is the strongest theoretical foundation for how privacy as a state sustains social networks in which individuals thrive.

"Privacy as a state" emphasises that individuals attain personal flourishing within various social networks by communicating their subjective phenomenological experiences of privacy violations. As they navigate different contexts, individuals' privacy states shift, influencing their sense of inclusion in specific situations (Dourish & Anderson, 2006). The following examples illustrate how privacy as a dynamic state

of mind, one that varies in type and intensity across contexts, helps individuals in specific situations achieve personal flourishing.

In the context of OBA, consumers may experience a sense of privacy violation when advertisers use their behavioural data in ways that feel intrusive or misaligned with their expected privacy. Research suggests that these perceptions of privacy violation are more pronounced when dealing with less trusted retailers compared to trusted ones (Bleier & Eisenbeiss, 2015). This suggests that consumers are more socially included in trusted retailers. Moreover, demographic and characteristics of consumers influence their social engagement with OBA. For example, female consumers express greater privacy concerns in OBA than males, suggesting they may feel less included in the OBA environment (Smit et al., 2014). Promotion-focused consumers, who are motivated by achieving gains, are less concerned about privacy risks than prevention-focused consumers in OBA (Ozcelik & Varnali, 2019). This implies that promotion-focused consumers feel more included in OBA than prevention-focused consumers.

A similar dynamic of privacy turbulence can be observed in marital relationships, reflecting individuals' levels of interaction within those relationships. In marital contexts, privacy turbulence may occur when one partner discloses private information without the other's consent. Whether privacy turbulence emerges and its intensity depends on the couple's established privacy boundaries, which are shaped by

the nature and status of their relationship (Petronio, 1991). This example illustrates the existence form of privacy states, which can feel intrusive or uncomfortable, and their varying levels are shaped by relational dynamics and contextual factors. Such variations reinforce the notion that privacy is a dynamic state that evolves with social interactions.

Another key aspect of privacy's social values, as discussed by Hull (2015), is its role in subjectification. Foucault (1982) defines subjectification as "the various ways in which individuals in our culture are made into subjects (p. 208)". This concept involves the "mode" of subjection, which is "the way in which the individual establishes his relation to the rule and recognises himself as obliged to put it into practice (Foucault, 1985, p. 27)". A core question in this process in privacy settings is: "Do I have more privacy or less?" (Hull, 2015). Privacy as a state aligns with the perspective by asking, "Do I feel more privacy or not? What feelings do I have?". The process of subjectification is particularly evident in contexts where individuals perceive a privacy intrusion.

For instance, in OBA, individuals experience a sense of lost ownership of privacy (Aguirre et al., 2015). Similarly, individuals feel turbulent when there is a breakdown in information control, particularly in high-stress situations such as bereavement (Basinger et al., 2016), handling parental infidelity (Thorson, 2015), feeling caught in

stepfamily dynamics (Afifi, 2003), sexting (Walrave et al., 2018), and social media use (Petronio & Child, 2020). These various privacy states in OBA and high-stress situations indicate that individuals exhibit different "modes" of subjection when engaging with diverse circumstances (Petronio & Child, 2020).

Ultimately, privacy's social value is embedded in how individuals interpret and navigate their interactions within social networks. Conceptualising privacy as a state illustrates that individuals respond to privacy-involved situations by adjusting their privacy expectations. Whether in OBA, marital relationships, or high-stress situations, individuals' privacy states reflect their inclusion levels and social bonds in the situations. Furthermore, the variability of privacy state across different contexts highlights the role of subjectification, demonstrating how individuals are socially subjected to privacy situations. By framing privacy as a fluctuating state, this approach provides a deeper understanding of its function in both individual flourishing and the maintenance of social networks.

4.4 Implications of Privacy Definitions Critical Review: Redefining Privacy as a State

This section critically examined privacy conceptualisations, highlighting key limitations of privacy conceptualisations in Smith et al.'s (2011) framework. Defining

privacy as a right fails to specify its core nature, while viewing it as a commodity oversimplifies its complexities. The widely accepted notion of "privacy as control" is increasingly impractical in the digital age, where users have little real control over their data (Büchi et al., 2022; Strycharz & Segijn, 2022). In contrast, "privacy as a state" offers a more dynamic perspective, capturing privacy as a subjective experience shaped by self-ego, environmental, and interpersonal factors (Laufer & Wolfe, 1977).

These insights call for a shift in privacy research from its original conceptual notion to a more social and psychological approach- privacy as a state. For instance, when examining privacy, particularly in digital contexts, the conceptualisation should shift from viewing privacy as control to understanding it as a state.

4.5 Privacy Concerns Measurements Critical Appraisal

In previous discussions, it is apparent that different definitions lead to different understandings of privacy. In response to Stern et al.'s (2001) argument that poor definitions would cause deficient measurements, this section examines whether OBA privacy scales are definition-driven. Specifically, my examination of these scales focuses on the following question: Which of the previous privacy conceptualisations do they meaningfully capture, and do they sufficiently assess it? In doing so, this

section aims to complete the critical evaluation of privacy conceptualisation, particularly in terms of control.

4.5.1 Conceptual Redundancy in Existing Privacy Scales

When examining the privacy scales in Table 1, I found the first concern with the theoretical and definitional underpinnings of privacy research. Specifically, it became apparent that there is considerable overlap between the different instruments, despite different terminology being used to describe the same concepts. For example, Li (2011) commented that "abuse" in Scale 3 deals with "improper access" and "unauthorised use" dimensions in Scale 1 (p. 459). This is an example of what Singh (1991) refers to as conceptual redundancy, where "theoretical justification is not available to view two constructs as logically different conceptualisations" (p. 256). Conceptual redundancy is associated with many problems for research and theory, most notably the "unnecessary proliferation of constructs" which hinders the process of systematic and cumulative research (Singh, 1991, p. 256). As with the definition of privacy, the conceptual redundancy reflects that there are varied definitions of the core concepts on which the privacy concept is built (or there would be consistent nomenclature). As such, I broadened the examination of the scales to remove conceptual redundancies, and thus unify some of the key terminology used in privacy research. This consolidation results in four dimensions, and each of these dimensions

uses a formal definition taken from prior literature and thus provides a more robust foundation for future research (see Table 3).

Table 3. *The consolidated privacy dimensions and related items*

Dimensions of Privacy	Definitions	Elements	Items	Scales
State	The "state" dimension refers to people's different psychological states, which link to how an individual feels about whether and how much their privacy has been invaded in a specific privacy situation.	Privacy being invaded	(1) When I am online, I have the feeling of being watched. (2) When I am online, I have the feeling that all my clicks and actions are being tracked and monitored.	Dinev and Hart (2004)/scale 3
Values (of)	The "values" dimension captures the underlying beliefs that consumers give to the third party's privacy protection approaches, their disposition to value privacy, their exposure to the situation, and the usage of their information.	General privacy	(1) Consumer online privacy is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared. (2) Consumer control of personal information lies at the heart of consumer privacy. (3) I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction. (4) It is very important to me that I am aware and knowledgeable about how my personal information will be used.	Malhotra et al. (2004)/scale 2
		Exposure	(1) Companies send too much advertising material. (2) Too many companies call to sell products and services.	Dolnicar and Jordaan (2007)

	(3) I receive too much advertising material.	
Data misuse	(1) I believe that companies use information for other purposes. (2) Consumer information is misused.	Dolnicar and Jordaan (2007)/ Scale 4
Data storage	(1) Information is safe while stored in a company's records.	Dolnicar and Jordaan (2007)
Data (unauthorised) sharing	(1) Companies share information with others without permission. (2) Companies regularly share information with others to offer products.	Dolnicar and Jordaan (2007)
Privacy protection	(1) Companies should devote more time and effort to preventing unauthorised access to personal information. (2) Computer databases that contain personal information should be protected from unauthorised access-no matter how much it costs. (3) Companies should take more steps to make sure that unauthorised people cannot access personal information in their computers. (4) Companies should not use personal information for any purpose unless it has been authorised by the individuals who provided the information. (5) When people give personal information to a company for some reason, the company should never use the information for any other reason. (6) Companies should never sell the personal information in their computer databases to other companies. (7) All the personal information in computer databases should be double-checked for accuracy-no matter how much this costs.	Smith et al. (1996)/scale 1

			(8) Companies should take more steps to make sure that the personal information in their files is accurate. (9) Companies should have better procedures to correct errors in personal information. (10) Companies should devote more time and effort to verifying the accuracy of the personal information in their databases. (11) When people give personal information to a company for some reason, the company should never use the information for any other reason.	
			(1) Companies seeking information online should disclose the way the data are collected, processed, and used. (2) A good consumer online privacy policy should have a clear and conspicuous disclosure.	Malhotra et al. (2004)
			(1) Companies must have privacy protection policies. (2) Companies should have privacy protection policies. (3) Companies should have privacy protection policies indicating reasons for protection. (4) Policies should indicate how they will protect information. (5) Government should restrict information collection. (6) Government should do more to protect safety of information. (7) Government should limit companies use of information.	Dolnicar and Jordaan (2007)
Attitudes (towards)	The "attitudes" dimension assesses how worried, afraid, uncomfortable, or bothered	Data collection	(1) It usually bothers me when companies ask me for personal information. (2) I'm concerned that companies are collecting too much personal information about me.	Smith et al. (1996)

	individuals are about the potential risks they might encounter and all perspectives of information usage.		(1) It usually bothers me when online companies ask me for personal information. (2) It bothers me to give personal information to so many online companies. (3) I'm concerned that online companies are collecting too much personal information about me.	Malhotra et al. (2004)
		Data misuse	(1) I am concerned that the information I submit on the Internet could be misused. (2) I am concerned about submitting information on the Internet, because of what others might do with it. (3) I am concerned about submitting information on the Internet, because it could be used in a way I did not foresee.	Dinev and Hart (2004)
			(1) I am concerned about misuse.	Dolnicar and Jordaan (2007)
		Data storage	(1) I am concerned that a person can find the following information about.	Dinev and Hart (2004)
			(1) I fear that personal information may not be safe while stored.	Dolnicar and Jordaan (2007)
		Data (unauthorised) share	(1) I feel uncomfortable when companies share information.	Dolnicar and Jordaan (2007)
		Potential risks	(1) When I shop online, I am concerned that the credit card information can be stolen while being transferred on the Internet.	Dinev and Hart (2004)
			(2) I don't mind receiving telephone calls. (3) Pleased to receive information from unfamiliar companies. (4) Consumers are not interested in getting information from unfamiliar companies.	Dolnicar and Jordaan (2007)

Behavioural intentions	The "behavioural intentions" dimension measures how people are inclined to act in a private setting.	Disclosure information	(1) When companies ask me for personal information, I sometimes think twice before providing it.	Smith et al. (1996)
			(1) When online companies ask me for personal information, I sometimes think twice before providing it.	Malhotra et al. (2004)
		Non-disclosure behaviour	(1) I request company to remove information if misused. (2) I request removal of information if sold to others. (3) I would support a company's effort to ensure safety. (4) I refuse to provide personal information without a reason supplied.	Dolnicar and Jordaan (2007)

4.5.2 A Thematic Framework for Consolidated Dimensions of Privacy

My approach to the consolidation was to follow Li's (2011) lead, where I compared the dimensions of privacy and the items in each prior privacy scale using thematic analysis to organise the data. To illustrate, the item "I have the feeling of being watched" reflects *a state* of privacy and was therefore categorised under the "state" dimension. I define the "state" dimension as people's different psychological states, which link to how an individual feels about whether and how much their privacy has been invaded in a specific privacy situation.

When items attempt to convey an individual's viewpoint on some aspects of privacy, I categorise them under the "values" dimension. For instance, items similar to "Companies should have privacy protection policies" ask respondents their thoughts on privacy protection. The item "It is very important to me that I am aware and

knowledgeable about how my personal information will be used" asks respondents about their beliefs of disposition to value privacy (Gironda & Korgaonkar, 2018). The items related to "Companies send too much advertising material" ask respondents about their beliefs about their exposure in the current situation. The other items asked respondents about their beliefs about information use. Notably, in the context of privacy, information use refers to how data may be misused, stored, or shared (Dolnicar & Jordaan, 2007; Smith et al., 1996). Thus, these items fall under the "values" dimension, which refers to "the underlying beliefs that consumers give to the third party's privacy protection approaches, their disposition to value privacy, their exposure to the situation, and the usage of their information".

I categorised items that assess how worried or bothered online users feel about various aspects of information usage under the "attitudes" dimension. Examples include statements like, "It bothers me to give personal information to so many online companies" and "I'm concerned that online companies are collecting too much personal information about me". As a result, I define the "attitudes" dimension as assessing how worried, afraid, uncomfortable, or bothered individuals are about the potential risks they might encounter and all perspectives of information usage.

I also categorised the items aiming to measure how online users intended to act in a private setting under the "behavioural intentions" dimension. I further concluded that

there are two universal behaviours in the privacy context: disclosure behaviour and non-disclosure behaviour. Therefore, my consolidation resulted in four consolidated broad privacy dimensions (e.g., “state”, “values”, “attitudes”, and “behavioural intentions”, see Table 3).

It has been emphasised that this is an initial consolidation, but the result is parsimonious and resolves a widespread concept redundancy problem while providing clear definitions for each dimension (see Table 4). Although this is an initial thematic consolidation, the four dimensions are exemplified in Westin (2003) and Laufer and Wolfe (1977) privacy theories. Westin (2003) definition of an individual’s privacy sits on four psychological states: solitude, intimacy, anonymity, and reserve, reflecting the state dimension. The behavioural intentions dimension reflects the actions individuals wish to take based on their privacy states, such as seeking solitude during downtime, enjoying the companionship of a close friend, or sharing personal matters with a stranger.

Table 4. *The connections between the consolidated four dimensions and non-OBA scales*

Non-OBA scales	**Dimensions**	**Connections to the consolidated four dimensions**

Westin (2003)	Westin (2003) identified that an individual's privacy sits on four psychological states: solitude, intimacy, anonymity, and reserve. A person may (1) want to be completely alone in downtime; (2) may want (or even desperately need) the companionship or sustaining presence of an intimate friend; (3) may want to open problems or situations to a stranger.	(1) State (e.g. "solitude, intimacy, anonymity, and reserve") (2) Behavioural intentions (e.g. "a person may want to do…")
Laufer and Wolfe (1977)	Laufer and Wolfe's (1977) theory claims that privacy has self-ego, environmental, and interpersonal dimensions. (1) The self-ego dimension refers to "a developmental process that, in our society, focuses on individuation (autonomy) and, by implication, personal dignity" (Laufer & Wolfe, 1977, p. 26)". This developmental experience involves a critical aspect to the relationship between the self (autonomy) and privacy: "I felt independent," "I could do what I wanted to do," "I could have my own opinions." (Laufer & Wolfe, 1977, p. 27). (2) The environmental dimension is composed of a series of elements that act as boundaries of meaning and experience. Environmental elements critically influence the individual's ability to perceive, have, and use available options. (3) Interpersonal dimension refers to that "privacy presupposes the existence of others and the possibility of a relationship with them." The four most frequent meanings of privacy were: aloneness, controlling access to information, controlling access to spaces, and "no one bothering me."	(1) State (e.g. "aloneness") (2) Attitudes (e.g. "I felt …") (3) Values (e.g. "I could do …") (4) Behavioural intentions (e.g. "controlling access to…")

Additionally, Laufer and Wolfe (1977) critical examination of the relationship between the self and privacy is demonstrated in statements such as, "I felt independent", "I could have my own opinions", and "I could do what I wanted to do". These statements correspond to the dimensions of attitudes, values, and behavioural intentions respectively. Therefore, despite the lack of empirical tests for the consolidated dimensions of information privacy, they could serve an important

function in highlighting existing issues regarding the conceptualisation and measurement of information privacy as control.

4.6 Implications of Privacy Measurements Critical Review: Redefining Privacy as a State

The consolidated dimensions clarify an inconsistency between the conceptualisation of information privacy as control and its existing measurements. However, the issues run deeper. When examining the consolidated dimensions of privacy, it's apparent that many of the dimensions are not truly privacy-related but are instead antecedents of privacy states and this serves to illustrate the utility of viewing privacy as a state. In particular, it's unclear how values can be seen as a part of privacy, as people have values which impact their views on any number of issues. For example, consumers' disposition to value privacy has been demonstrated to be a positive predictor of their privacy concerns (Gironda & Korgaonkar, 2018; Stanaland et al., 2011). Therefore, it's apparent that an individual's valuation of privacy is not a dimension of privacy itself, but rather an antecedent that will influence a person's sense of their state of privacy. In the case of attitudes, these are again antecedents to a state of privacy. For example, a concern about the misuse of information is one of many factors influencing a consumer's perception of their privacy state, such as when they visit a website without a privacy policy. Similarly, behavioural intentions stem from attitudes and values, which could be called intended privacy-responsive behaviour. However,

they do not constitute privacy itself. In summary, much of the existing research appears to focus on antecedents to privacy states, rather than on privacy itself. While studying these antecedents is important, it's also important to distinguish them as what they are as antecedents, not privacy itself.

If looking at the back of the analysis of privacy definitions, it can be found that "control" is also an antecedent that leads to a state of privacy. This argument has been supported by existing privacy theories. For instance, Laufer and Wolfe's (1977) dimensions of privacy provide useful perspectives on the core of privacy which is a sense of control over personal (or group) information. This is further bolstered by Koops et al. arguing that control is an overarching antecedent to perceptions of a state of privacy. Similarly, Petronio's (2020) communication privacy management theory shows that a breakdown in information control results in a state of "privacy turbulence." The idea of privacy as a state of mind determined by control allows me to confirm that privacy is not control but a *state*, and people's perception of the degree of control over sensitive personal/group information is a factor that shapes people's privacy state.

In summary, privacy is a state shaped by various factors, such as perceived control over information, privacy values, and attitudes towards all perspectives of using information. This view extends beyond seeing privacy as control of a set of

mechanisms or rules for information use. As a result, the results of the examination on privacy measurements show that "privacy as a state" is a practical solution to the theoretical challenges surrounding privacy measurements. These findings respond to the implication of the examination of privacy definition: a call for a shift in privacy research from its original conceptual notion (mainly privacy as a control) to a more social and psychological approach- privacy as a state.

4.7 Applying A Transition from Defining Privacy as Control to a State in OBA

Both the results of examinations on privacy definitions and measurements point to a transition to defining privacy as a state from its original conceptual notion, this section aims to make a logical case of how the transition from defining privacy as control to a state applied to the context of OBA. As I argued before, the predominant conceptualisation approach of privacy is "privacy as control"; this section will examine the limitations of control-based privacy definitions in the context of OBA and argue that conceptualising privacy as a state offers a more comprehensive approach.

4.7.1 Limitations of Control-Based Privacy in OBA

As discussed in previous discussion, OBA research defined consumer privacy as information privacy (Baek & Morimoto, 2012; Bleier & Eisenbeiss, 2015; Gironda &

Korgaonkar, 2018; Ham, 2017; Jung, 2017; Kim & Huh, 2017; Li, 2011). As such, the conceptualisation of information privacy in OBA has at the core concept of personal information control- that it is about who gathers and disseminates consumer information under the circumstances of OBA (Li, 2011; Smith et al., 1996; Westin, 1968). However, this control-based privacy conceptualisation in OBA is theoretically limited.

The success of OBA relies on online tracking technologies like cookies, which are complex and often not fully understood by consumers (Ham & Nelson, 2016; Smit et al., 2014). Although online advertisers provide a form of cookie consent (Zarouali et al., 2017), the technological complexity creates an asymmetry of OBA and consumer knowledge (Hull, 2015), fundamentally limiting consumers' ability to exercise information control. This indicates that consumers are not in control of their informational transactions with advertisers. Therefore, defining consumer privacy as information control in OBA is fundamentally a theoretical illusion.

Furthermore, regarding the privacy concerns scales utilised in OBA studies, as I argued before, existing privacy concerns scales embedded the conceptual redundancy issue; thus, adapted privacy concerns scales in OBA also fail to measure consumers' perceptions of control or their ability to control, but values of privacy and attitudes towards information usage. For example, the item "It bothers me to receive too much

advertising material of no interest" in scale 5 assesses consumers' attitudes towards advertising, and the item "I believe that personal information is often misused" asks consumers' values on information usage.

4.7.2 Privacy as a State in OBA

The chapter previously proposes that privacy should be understood as a heterophenomenological phenomenon, allowing people to describe their perception of a privacy state in a given context. This approach has been supported by several OBA empirical studies. For example, when confronted with OBA, Aguirre et al. (2015) demonstrate that privacy is something consumers "own" in OBA i.e. when consumers recognise that their ownership of privacy has been exploited, they experience a state of loss of ownership of privacy. Similarly, Phelan et al. (2016) found that consumers describe their feelings about this privacy intrusion as "acceptable", "annoying", "weird", "creepy", "disturbing", or "risky" (Phelan et al., 2016). Empirical evidence of these varied consumer reactions in OBA confirms that privacy is a state of mind.

In conclusion, the theoretical limitations of defining privacy as control in the context of OBA, alongside the empirical findings on privacy states, support the transition toward conceptualising privacy as a state in this context. Most importantly, whilst OBA research provides only a preliminary demonstration of several privacy states in

OBA, its significance as a representative privacy-involved context in the digital age reinforces the validity of conceptualising privacy as a state.

4.8 Conclusion and Implications

This chapter critically examines existing privacy definitions and measurements. The results reveal that, except for privacy as a state, other strides of privacy conceptualisation, particularly the control-based conceptualisation of privacy, are embedded with obvious theoretical illusions. Further, the privacy measurements have also been found redundant and insufficient in measuring privacy as control, rather than their states, attitudes, values, and behavioural intentions.

The chapter makes a logical case for how conceptualising privacy as a state more accurately captures the subjective and psychological nature of privacy experiences. This conceptualisation not only brings greater definitional clarity but also highlights its social value. By framing privacy as a state, the concept becomes more coherent and adaptable, taking into account individuals' perceptions of control over their information. Moreover, this conceptualisation underscores privacy's essential role in fostering self-flourishing and modes of subjectification, thereby enhancing its social significance.

Reconceptualising privacy as a state introduces a more flexible and comprehensive framework for understanding privacy in various contexts. The exploratory application of this shift in the context of Online Behavioural Advertising (OBA) demonstrates that moving from a control-based to a state-based perspective has significant implications OBA practices. This transition challenges the traditional emphasis on control and instead advocates for a deeper exploration of individuals' perceptions and psychological states surrounding privacy.

In conclusion, defining privacy as a state provides a robust, adaptable theoretical framework for understanding privacy. This new conceptualisation sets the stage for future theoretical and empirical inquiry, offering fresh avenues for exploration and a clearer lens through which to examine privacy in an increasingly digital world.

Chapter 5: Empirical Privacy Research in OBA – Critical Appraisal

5.1 Introduction

The overview in Chapter 3 highlights the fragmentation and conflicting empirical findings associated with consumer privacy concerns. Such issues hinder the development of a comprehensive understanding of consumer privacy concerns in OBA. To address these issues, it is crucial to examine the underlying reasons for these issues. As such, a critical examination of the empirical privacy research in OBA warrants a separate chapter for further clarification. This examination clarifies the precise impact of factors which lead to conflicting results and informs the theoretical understanding and applications of consumer privacy in OBA.

The following section critically examines empirical privacy research in OBA focusing on key questions: Are the research results inconsistent? Do they align with, support, or challenge existing privacy theories? Guided by these criteria, several key issues have been identified.

5.2 Confounding Contextual Variables in Defining Privacy

As Mowday and Sutton (1993) argue, both external contextual variables and individual social factors play influential roles in shaping privacy concerns. Following this perspective, many antecedents of consumers' privacy concerns in OBA could be

broadly treated as contextual variables. However, a closer examination reveals important distinctions that merit deeper attention.

Among the ad-controlled antecedents, ad personalisation and ad context stand out as key external variables. The impact of ad personalisation on consumer privacy concerns has been consistently significant: highly personalised OBA often triggers greater consumer concerns about privacy (Bleier & Eisenbeiss, 2015, Aguirre et al., 2015, Van Doorn and Hoekstra, 2013). Yet, digging deeper, the effects of ad context present a more complex picture. As discussed in Chapter 3, perceived personalisation's influence on privacy concerns varied across different contexts. Specifically, while OBA has little to no effect on privacy concerns in news context, it has a slight impact in commerce and health contexts (Bol et al., 2018) and a significant impact in political contexts (Turow et al., 2012). These findings underscore a crucial point, that is, the external context in which ads appear matters greatly and must be prioritised when considering consumer privacy concerns.

Turning to consumer-related antecedents, the review shows that demographic factors consistently predict privacy concerns (Smit et al., 2014). However, the role of cultural norms introduces additional complexity. Research has revealed inconsistent findings regarding the effect of consumer knowledge on privacy concerns, varying from region

to region, suggesting that cultural norms may moderate this relationship (Brinson & Eastin, 2016; Ham, 2017; Smit et al., 2014; Strycharz et al., 2019; Wohn et al., 2015).

The possibility that cultural norms moderate these effects is critical. It suggests that consumer-related factors are not contextual variables themselves but are better understood as inputs that interact with ad-controlled characteristics to shape privacy concerns. This insight challenges the notion that individual social factors should be treated as contextual variables in their own right. Instead, when examining how contextual factors in OBA influence privacy concerns, individual social factors, such as demographics, culture, and knowledge, should be identified and assessed as antecedents rather than as context.

Thus, the central issue with confounding contextual variables lies in the need to clearly distinguish between external contextual factors and individual social factors. These two types of influences play fundamentally different roles in influencing individual privacy, and should not be grouped together, as Mowday and Sutton (1993) suggest. External contextual factors should be recognised as the platforms that frame privacy experiences, whereas individual social factors form the foundations that shape privacy concerns within those frames.

5.3 Misspecification of Cognitive Appraisal Variables

One of the most controversial antecedents in the study of consumer privacy concerns within OBA is the cognitive appraisal process, particularly the constructs of threat appraisal and coping appraisal. In the context of OBA, threat appraisal, which involves consumers' evaluation of perceived risks and benefits, has been studied as a predictor of consumer privacy concerns (Ham, 2017; Phelan et al., 2016). However, as highlighted in the review, empirical findings regarding the role of perceived benefits have been highly inconsistent (Ham, 2017; Jung, 2017; Palos-Sanchez et al., 2019; Wohn et al., 2015). I argue that these contradictions arise from a misspecification of the perceived benefits variable: consumers' perceived benefits are not theoretically appropriate predictors of privacy concerns in privacy contexts.

This inconsistency can be traced back to the theoretical origins of threat appraisal. The "threat appraisal" construct, originally used to explain individuals' perceived threats in risky environments (Ham, 2017), aligns with Wolfe and Laufer's (1971) concept of "privacy calculus" in privacy situations. Privacy calculus suggests that individuals weigh benefits against privacy risks to inform privacy behaviours, not necessarily the formation of privacy concerns (Laufer & Wolfe, 1977). Misspecifying perceived benefits as directly influencing privacy concerns leads to conceptual confusion and fragmented empirical outcomes. Thus, perceived benefits should be

more appropriately linked to privacy behaviour rather than to privacy concerns themselves.

A similar pattern of misapplication appears in research on the variables assessing coping appraisal, an individual's ability to implement coping responses (Ham, 2017). As highlighted in the review, findings regarding the effect of self-efficacy on privacy concerns have been particularly inconsistent (Ham, 2017; Wohn et al., 2015), further indicating a misspecification conceptual problem. These contradictions arise from the misspecification of the variables of coping appraisal. The primary purpose of coping appraisal is to explain individuals' perceptions of self-protection in risky environments (Ham, 2017). In this regard, coping appraisal factors should explain consumers' perceived self-protective capacities rather than their level of privacy concern. As such, when coping appraisal is linked directly to privacy concerns, it represents a misspecification, which distorts the theoretical relationships and undermines cumulative research progress.

Notably, consistent evidence shows that privacy concerns significantly shape key cognitive perceptions, such as ad scepticism (Baek & Morimoto, 2012; Zarouali et al., 2017), perceived intrusiveness (Gironda & Korgaonkar, 2018; Mpinganjira & Maduku, 2019; Van Doorn & Hoekstra, 2013), and perceived risk (Yang, 2013). These findings highlight the misspecification of cognitive appraisal in privacy concerns and suggest a reversed causal pathway: instead of threat and coping appraisals predicting

privacy concerns, it is privacy concerns that influence individuals' threat perceptions and protective evaluations within OBA environments.

In sum, the critical issue with the cognitive appraisal variables lies in their misspecification of privacy concerns. Properly theorising the relationships suggests that privacy concerns act as a driver, not an outcome, of consumers' cognitive appraisals in OBA. This insight provides an essential corrective for developing more accurate and coherent models of consumer privacy decision-making.

5.4 The Missing Trade-Offs

When examining the behaviours influenced by consumer privacy concerns, it becomes apparent that the findings are fragmented and inconsistent. While privacy concerns have been shown to influence purchase intentions (Van Doorn & Hoekstra, 2013), ad avoidance (Baek & Morimoto, 2012; Ham, 2017; Jung, 2017) and, to some extent, click intentions (Bleier & Eisenbeiss, 2015), they do not appear to significantly affect opt-out behaviours (Strycharz et al., 2019) or self-disclosure behaviours (Bol et al., 2018).

Moreover, even among behaviours where an effect is found, results are not fully consistent. For example, Nyheim et al. (2015) reported that privacy concerns did not significantly predict ad avoidance when accounting for variables like perceived

control and gender among Millennials. Moreover, while Bleier and Eisenbeiss (2015) found that privacy concerns negatively affect click intentions, both Kim and Huh (2017) and Gironda and Korgaonkar (2018) found no significant effects between privacy concerns on consumers' intentions to click on ads.

These fragmented and inconsistent findings highlight a deeper conceptual issue: the problematic assumption of a direct cause-and-effect relationship between privacy concerns and behaviour. According to Laufer and Wolfe (1977), privacy behaviours are not a straightforward outcome of privacy concern alone. Instead, behavioural decisions emerge through a trade-off process, where individuals balance perceived risks and benefits before acting in a privacy context. Without properly considering this trade-off mechanism, attempts to link privacy concerns directly to behaviours risk oversimplifying the complex decision-making process consumers engage in.

Thus, I argue that privacy concerns should not be treated as a direct predictor of behaviour. Instead, the role of trade-offs must be central to understanding privacy behaviours. The absence of this consideration in the OBA literature likely explains the observed fragmentation and inconsistency in behavioural outcomes. Recognising and incorporating the prerequisite role of trade-offs is therefore critical for advancing a more coherent and accurate understanding of privacy behaviours in online advertising settings.

5.5 Shaky Mediator

Given the above critical analysis, it becomes evident that positioning consumer privacy concerns as a mediator is theoretically problematic. As noted, Ham (2017) demonstrated privacy concerns mediating the effects of perceived risk and self-efficacy on ad avoidance. However, this formulation reflects fundamental misspecifications and the missing trade-off.

Again, perceived risk is inherently part of trade-off perceptions; it should not be treated as an antecedent of privacy concerns. Instead, it should be treated as an outcome of privacy concerns and the predictor of consumer behaviour (e.g, ad avoidance). Similarly, self-efficacy, a core component of coping appraisal, should not conform to privacy concerns.

Moreover, as previously argued, privacy concerns should not directly predict behaviours, such as ad avoidance, without accounting for trade-off evaluations. Modelling privacy concerns as a mediator between perceived risk, self-efficacy, and ad avoidance in this way misrepresents the underlying mechanisms and oversimplifies the decision-making process. Thus, the claimed mediation effect is theoretically shaky.

5.6 Conclusion and Implications

The review of empirical research on consumer privacy concerns in OBA (Chapter 3) reveals a fragmented and often inconsistent landscape regarding both the antecedents and outcomes of privacy concerns. Considering the importance of cognitive success (Niiniluoto, 1999) in empirical research, this chapter critically examines the underlying issues contributing to this fragmentation and the inconsistencies. Specifically, it has highlighted key theoretical issues: the confounding contextual variables in defining privacy, the misspecification of cognitive appraisal variables, the missing trade-offs in examining privacy behaviour, and the theoretically shaky positioning of privacy concerns as mediators between cognitive appraisals and behaviours. These unresolved theoretical issues continue to cloud a coherent understanding of consumer privacy concerns in OBA, while their critical analysis opens up valuable points for rethinking how privacy concerns operate in OBA.

The discussion in Section 5.2 underscores the importance of properly distinguishing contextual variables. Rather than treating all antecedents equally, external factors (such as ad personalisation and ad context) should be seen as platforms that set the stage for privacy concerns, while individual social factors (such as demographics and cultural norms) must be recognised as the antecedents that shape these concerns.

Sections 5.3 and 5.4 emphasise the centrality of trade-offs in understanding privacy behaviours. Privacy behaviours do not arise directly from privacy concerns alone; rather, they emerge through a trade-off process where individuals weigh perceived risks against benefits. To avoid cognitive failure by overlooking this crucial mechanism, it is essential to demonstrate that trade-offs occur before privacy behaviours are engaged.

Taken together, these insights point toward the need for a more robust theoretical framework. I propose the following foundation for understanding consumer privacy concerns in OBA:

Consumers may broadly express concerns about privacy, or not, depending on situational contexts (e.g, OBA personalisation), influenced by personal social factors. These privacy concerns then shape an actual trade-off between perceived benefits and risks, which in turn influences their behaviour.

This framework offers a conceptually valid and theoretically coherent starting point for developing a new privacy model in the context of OBA, which addresses the problems identified throughout this critical appraisal.

However, advancing this framework into a fully developed model is not a straightforward task. Beyond critically examining privacy definitions and empirical evidence, a crucial next step involves critically evaluating existing privacy models and frameworks which are also developed within empirical traditions. This examination is necessary not only to identify valuable elements that could enrich the new model but also to rigorously assess whether current models adequately account for contextual variables, the role of trade-offs, and the connection between privacy concerns and behaviour.

Chapter 6: Privacy Models – Critical Appraisal

6.1 Introduction

Building on the discussion in Chapter 5, which highlighted key theoretical issues in empirical research on consumer privacy concerns in OBA, this chapter turns to a critical examination of whether existing privacy models and frameworks, which are developed within empirical traditions, have considered these limitations.

This chapter examines four key privacy models: (1) Smith et al.'s (2011) Antecedents-Privacy Concerns-Outcomes (APCO) model; (2) Li's (2011) Integrative framework on Concerns for Information Privacy (CFIP); (3) Trepte's (2021) the social media privacy (SMP) Model; (4) Dienlin's (2014) privacy process model (PPM). The examination of these models focused on the following questions: Are the models parsimonious, are they a complete explanation regarding context and trade-offs, and are they founded on a clear definition of privacy?

These questions serve to assess how well each model aligns with the conceptualisation of privacy as a state introduced in Chapter 4, and with the theoretical insights critically proposed in Chapter 5. The overall conclusion is that, although these models build on empirical insights and make valuable contributions, they operate without a clear conceptualisation of privacy as state and fall short in

addressing the theoretical fragmentation and inconsistencies previously identified. These shortfalls highlight the need for a more conceptually robust and practically applicable model of privacy in the context of OBA, one that synthesises the most insightful elements of existing models while addressing their conceptual gaps.

6.2 Selection of Privacy Models

To identify suitable privacy models for analysis, a literature review was conducted to research representative privacy frameworks across multiple disciplines. The review utilised Scopus and Google Scholar (GS) to search for keywords, abstracts and potentially relevant full-text articles. As in the selection of empirical research on consumer privacy in OBA discussed in Chapter 3, Scopus was employed to ensure the inclusion of high-quality models, while GS was used to capture broader range of privacy frameworks (Meho & Yang, 2007).

The aim of this review was to identify a representative sample of earlier overarching privacy models/frameworks that focus on empirical findings related to individual privacy across diverse contexts. To this end, the following keyword search was employed: “information privacy”, “privacy”, “literature review”, “framework”, and “model”. The search was further restricted to the disciplines of Computer Science, Social Sciences, Psychology, Arts and Humanities, in line with Stuart et al.’s (2019)

review of privacy literature. Within Computer Science, terms such as “Blockchain”, “Cloud Computing”, “Health Care”, “Smart City”, and “Medical” were excluded, as these domains technically have too narrow a focus on very particular aspects of privacy (Smith et al., 2011). As such, this process initially yielded 11 privacy models/frameworks for further evaluation, of which nine came from Scopus and two from the GS.

Following a detailed assessment, several models were excluded. The model proposed by Yun et al. (2019) was removed, as its primary aim is to generate research questions rather than explain privacy as a concept. Models that lack an empirical foundation, for example, Li (2012), or that examine privacy from a multi-level perspective (e.g. government, societal, and organisational) rather than from the standpoint of the individual were also excluded, for example, Bélanger and Crossler (2011) and Li (2014). Moreover, as the review seeks to explore privacy within a broader context, models focused on specific issues were omitted. This includes frameworks addressing the privacy paradox (Barth & De Jong, 2017), personalisation transparency (Segijn et al., 2021)and behavioural intention in the context of autonomous vehicles (Keszey, 2020). Applying these criteria, four key privacy models/frameworks were selected for further examination: (1) Smith et al.’s (2011) Antecedents-Privacy Concerns-Outcomes (APCO) model; (2) Li’s (2011) Integrative framework on Concerns for

Information Privacy (CFIP); (3) Trepte's (2021) the social media privacy (SMP) Model; (4) Dienlin's (2014) privacy process model (PPM).

6.3 Examinations of Privacy Models

6.3.1 Smith et al.'s (2011) Antecedents-Privacy Concerns-Outcomes (APCO) Model

Smith et al.'s APCO model is based on a wide range of normative and descriptive privacy studies (see Figure 2) and focuses on privacy *concerns* rather than privacy. They argue that privacy is not amenable to measurement, and thus, privacy concerns can act as a proxy for privacy. The problem with this formulation is that, whilst discussing privacy definitions, they never settle on a definition, and, as Jarvis et al. (2003) argue, it is necessary to define a concept before measuring it. Furthermore, the argument that privacy cannot be measured is problematic, as it is unclear what cannot be measured. In their review of privacy as a state, Smith et al. correctly identify that privacy as a state allows for a continuum of privacy from "absolute to minimal" (p.995). As people can understand and identify a state of privacy, it is a measurable concept when thus defined. Therefore, despite the model providing a valuable springboard for further ideas, it is hampered by measuring a proxy when it is better to examine the focal concept directly.

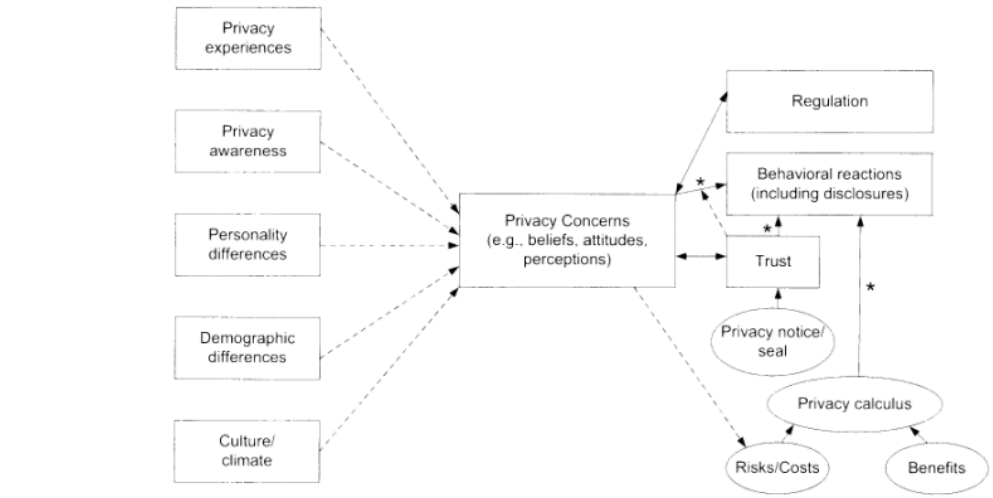


Figure 2. *Smith et al.'s (2011) Antecedents-Privacy Concerns-Outcomes (APCO) Model*

Nevertheless, the APCO model includes some key factors that are inputs into the perception of privacy; privacy experience, privacy awareness, personality differences, demographic differences, and culture/climate. As shown in Figure 2, these inputs result in three main outcomes (i.e., behavioural reaction, regulation, and trust), and the authors highlight the important role of privacy calculus. Of particular interest is their notion of the privacy paradox, an intention-behaviour gap (Sheeran et al., 2005), whereby intentions to retain privacy do not translate into actions. Even though people intend to maintain privacy broadly, this does not mean they will not trade their privacy for perceived benefits, and there is no paradox from this perspective. Instead, as per Laufer and Wolfe (1977), the behaviour-intention calculus, or rather the trade-off, takes place in a given context. Whilst the APCO model identifies relevant

antecedents and discusses the importance of context in relation to privacy, it does not incorporate the context in the model by arguing that a generalisable model is not possible if the context is included. However, aside from identifying a wide variety of potential contexts, no reason is provided that justifies why such an important determinant of behaviour should be absent from a generalised model. For example, even if only looking at the digital environment, context might still matter, e.g., a person with an urgent need to purchase an item might be more willing to trade off their privacy to obtain that item.

6.3.2 Li's (2011) Integrative Framework on Concerns for Information Privacy (CFIP)

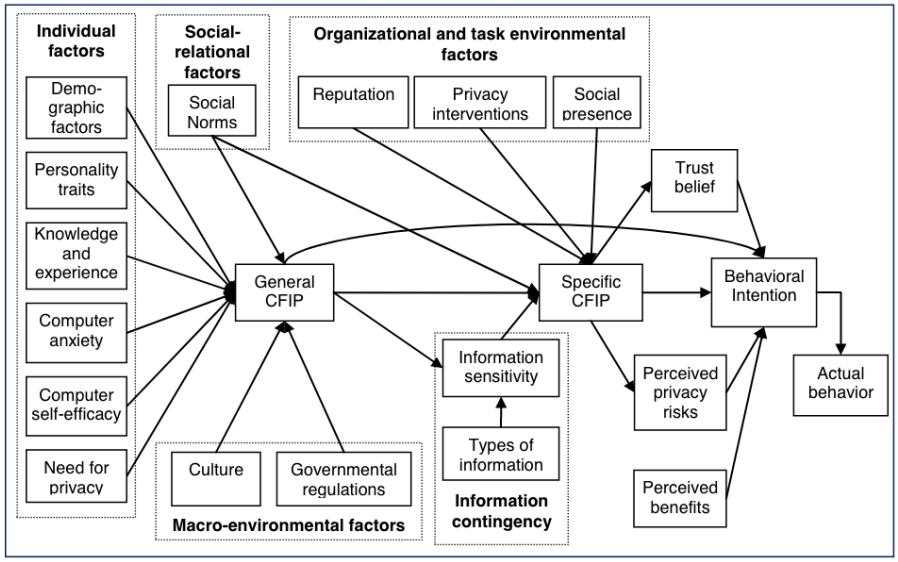


Figure 3. *Li's (2011) Integrative framework on Concerns for Information Privacy (CFIP)*

Li's (2011, see Figure 3) privacy model is based on a comprehensive review of relevant literature and is notable for the extensive number of antecedents that influence privacy (again, these insights have been applied to inform the development of the new model in Chapter 8). Li correctly identifies that an individual may have general concerns for information privacy (CFIP) and specific CFIP, which is Li's way of addressing the issue of context. Li correctly identifies a very loose connection between the general and specific CFIP; in effect, Li is making the point that general CFIP is subsumed under contextual factors if it is of any relevance. Again, people may broadly value privacy or not, but will change that value in a situational context of an actual trade-off. And in Li's model, a trade-off is implied but not explicitly specified, even though this must occur with the inclusion of risks and perceived benefits in the model (Laufer & Wolfe, 1977). In other words, the general CFIP is not a guide to the actual behaviour, and its value in understanding/predicting behaviour is questionable. Furthermore, the critical elements of perceived benefits are isolated from the wider model and appear without any antecedents or moderators. This is a problem. For example, prior experience with similar trade-offs will undoubtedly influence the perception of benefits. Finally, although Li's model provides some helpful detail on antecedents, the model lacks parsimony and may be seen as overly complex and difficult to follow.

6.3.3 Trepte's (2021) The Social Media Privacy (SMP) Model

In the context of media and communication studies, Trepte (2021) has developed a social media privacy (SMP) model (see Figure 4). Their model is built on a definition of privacy as control of information, and due to the interpersonal and communicative nature of social media, the SMP is predicated on individuals already having lost control over their privacy. Given that they have lost control over their personal information, all users can do is decide how their personal information can be communicated and what kind of personal information a person wishes to share. The model offers an interesting view of some specific aspects of social media and privacy, but, because it assumes a loss of control at the outset, it does not focus on the trade-offs that take place firstly in joining a platform, in what content to publish, or the facility of most social media platforms to choose who can access specific information. Further, if users' knowledge of social media and prior experience on a particular social media platform may be considered antecedents to online users' privacy experiences (Yang, 2013), so can other personal factors. As such, in the SMP, there needs to be a line between individual initial evaluation and people's subjective private experience. Moreover, the antecedents of people's subjective privacy experience should have been included in the model.

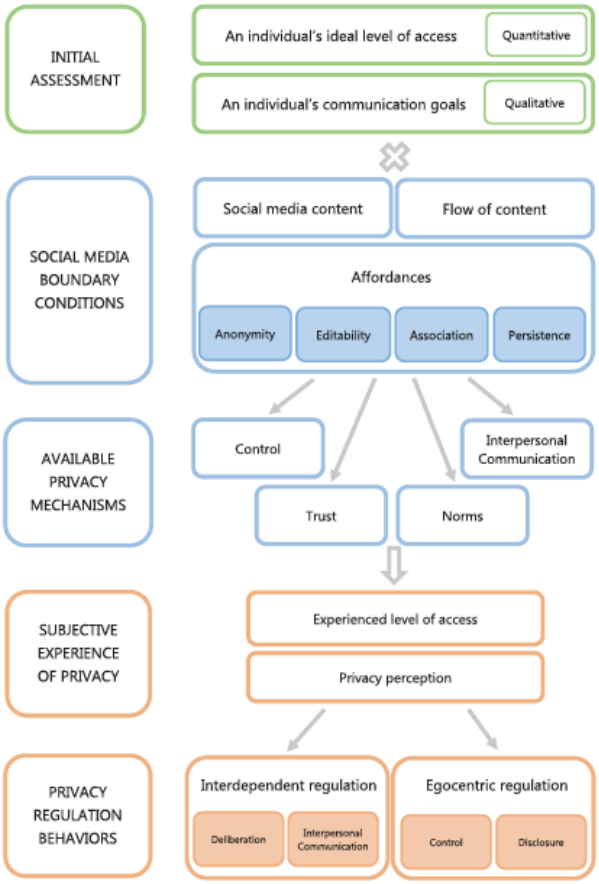


Figure 4. *Trepte's (2021) Social Media Privacy (SMP) Model*

Oddly, Trepte concludes that, on social media, "privacy is not a private affair. It is at the centre of communication. We are out of control because we have so much to share" (p.18). This conclusion rejects the notion that individuals make any trade-offs with their privacy. Whilst there are many examples of people sharing information that might best be kept private, for example, broadcasting death through Internet live streaming is a growing phenomenon worldwide, even in Western countries where privacy is highly valued (Fratini & Hemer, 2020), this does not mean that trade-offs are not taking place. In the example given, the disclosure of suicide, a highly private

issue, likely resulted from wishing to make their death more meaningful. Undoubtedly, social media encourages trade-offs with poor outcomes for people, but that does not mean they are not taking place. In summary, the model is hampered by an assumption that platform users are "out of control" when in control but may sometimes use that control poorly.

6.3.4 Dienlin's (2014) Privacy Process Model (PPM)

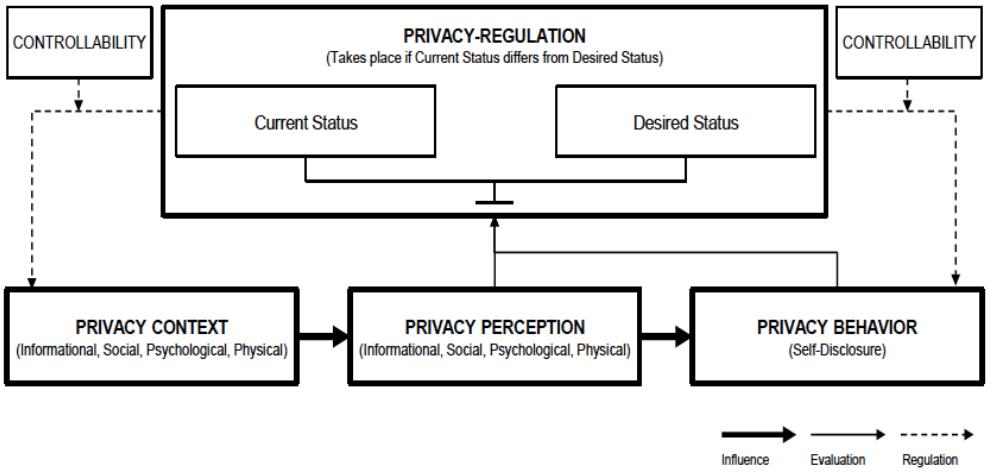


Figure 5. *Dienlin's (2014) Privacy Process Model (PPM)*

Dienlin's (2014, see Figure 5) privacy process model (PPM) has the notable feature that it proposes a "current status" of privacy and a desired status, which, although Dienlin does not define privacy, conforms with the idea of privacy as a state (Smith et al., 2011). However, the idea of desired status does not seem to conform to the obvious point that most people like to keep what they perceive as private unless there

is a benefit to disclosure. This points to the most significant drawback of the model: it does not include a trade-off in determining behaviour. When, for example, a person is asked to disclose information in return for some benefit, they do not desire a less private status; they are willing to trade some of their privacy for benefit *x*. Indeed, the PPM could include no privacy example, outside of coercion, where a privacy context does not include some kind of trade-off.

Dienlin provides an example of a desired less private status whereby a father has finished work and is having dinner with his family and seeks to decrease his privacy status by sitting closer to a family member to lower their privacy status. As an illustrative example, the privacy issue at hand is difficult to parse, and further, there is a likely benefit to a trade-off against less privacy with family (e.g., you cannot have intimacy without giving up privacy). Nevertheless, Dienlin does put great emphasis on the importance of context in shaping privacy-related behaviour and implicitly recognises that privacy is a heterophenomenological phenomenon.

6.4 Conclusion and Implications

This chapter critically examined four key privacy models, assessing their capacity to address the theoretical and empirical issues identified in preceding chapters. While

each model offers valuable insight into consumer privacy concerns, several notable limitations could be identified.

A key shortcoming shared across these models is the reliance on *privacy concerns* as a proxy for privacy itself. As previously discussed, attempting to measure privacy without a clear conceptualisation of what privacy is undermines the explanatory power of these models. Furthermore, while some models, such as Li's CFIP framework, make efforts to incorporate contextual elements, they fall short of integrating context into a cohesive platform for defining privacy. Similarly, the concept of trade-offs, central to understanding privacy-related behaviour, is either implicit (as in CFIP and APCO) or largely absent (as in SMP and PPM). In the absence of a clear consideration of how individuals weigh privacy risks against potential benefits, these models are limited in their ability to provide a comprehensive account of privacy behaviour.

In light of these shortcomings, this chapter underscores the need for a more integrative privacy model that explicitly incorporates (1) a robust and conceptually grounded definition of privacy, particularly privacy as a state; (2) the influence of contextual variables in shaping privacy concerns and behaviours, and (3) the role of trade-offs in shaping privacy behaviour. Nevertheless, these insights provide a foundation for the next stage of the research: developing a refined theoretical privacy

model/framework that incorporates the above essential elements and seeks to provide a more holistic understanding of consumer privacy in OBA.

Notably, whilst the above privacy models fall short in resolving the theoretical fragmentation and inconsistencies previously identified, they still offer valuable contributions to the development of a more refined privacy model/frameworks. Each model brings to light critical elements that inform both the antecedents and consequences of individual privacy concerns. For example, the APCO and CFIP models offer well-established frameworks for identifying personal, demographic, and cultural norms as key antecedents of privacy concern. Importantly, they also underscore the presence of trade-offs individuals make in the process of conducting intended behaviour.

In contrast, the SMP and PPM models move beyond individual-level factors, placing greater emphasis on the predictive influence of contextual conditions. The SMP model, for example, highlights how the social media boundary interacts with personal factors to shape users' subjective experience of privacy. Similarly, the PPM underscores the role pf broader privacy context in shaping privacy perceptions, even if it stops short of fully considering personal, demographic, and cultural norms.

These insights from prior privacy models/frameworks have played a crucial role in informing the development of a new, multi-dimensional yet parsimonious model of privacy. In doing so, the new model not only addresses key conceptual and empirical gaps left by existing privacy models but also builds on their systematic categorisation of relevant factors. Drawing from and organising these elements is not merely a recognised practice in model development; it is a necessary step to ensure theoretical coherence and practical utility.

A particularly relevant example is Boerman et al. (2017), who developed a framework for understanding empirical outputs about consumer responses to online behavioural advertising (OBA). Their model builds directly on the main factor categories outlined in Rodgers and Thorson's (2000) Interactive Advertising Model, systematically incorporating empirical variables from the OBA context to explain how these factors interrelate in shaping consumer behaviour. This precedent reinforces the importance of grounding new theoretical models in established conceptual structures while adapting them to address emerging empirical evidence. As such, the following chapter 8 provides a detailed account of how these insights converge in the construction of the new Contextual Privacy State model.

Chapter 7: Empirical Study: Privacy as a State

7.1 Introduction

While earlier chapters have conceptually argued that privacy should be understood not as control or commodity in OBA, but as a heterophenomenological state, such a redefinition requires empirical support to move beyond abstraction. To date, empirical evidence supporting the notion that individuals experience privacy as a state remains scarce (Aguirre et al., 2015; Phelan et al., 2016). Moreover, the few existing studies are not definition-driven, offering limited conceptual grounding for this perspective.

This chapter addresses that gap by empirically exploring whether privacy is indeed perceived as a state by individuals, particularly in the context of online behavioural advertising (OBA), and whether such experiences are consistent and generalisable across different privacy-relevant contexts.

To achieve this, a mixed-methods research design was adopted, integrating both qualitative and quantitative approaches. The qualitative phase draws on in-depth, semi-structured interviews to uncover the emotional and cognitive descriptors individuals use to articulate privacy experiences. These insights inform the subsequent quantitative phase, which tests the general applicability of those

descriptors across multiple contexts, including OBA, changing room surveillance, and interpersonal disclosure.

7.2 Structural Role of the Empirical Study

This chapter plays a critical role in the thesis. Although the overall aim of this research is *theoretical*, this empirical component provides essential evidentiary support for the proposed transition from prominent conceptions of privacy to a state-based approach. The findings presented here not only help validate the plausibility of this reconceptualisation but also contribute to the development of the Contextual Privacy State (CPS) framework, which is grounded in the conceptualisation of privacy as a state and will be introduced in later chapters. In this way, Chapter 7 serves as a vital empirical bridge between the thesis's conceptual foundation and its forthcoming theoretical developments in Chapter 8.

In relation to the overarching research question of the thesis: *Has consumer privacy been validly conceptualised in the context of OBA, and if not, what are the theoretical and empirical implications of this conceptual inadequacy?* The empirical study in this Chapter examines the empirical implications of the reconceptualisation of privacy as a state through two specific research questions. Specifically, the first research question (*Q1: What privacy states would consumers perceive in the context of OBA?*)

investigates what types of privacy states consumers perceive in the context of OBA, thereby empirically examining whether consumers' experiences of privacy in OBA are better understood as psychological states. The second research question (*Q2: Are the privacy states in OBA associated with other contexts?*) further explores whether these privacy states observed in OBA are associated with privacy experiences in other contexts to examine privacy's contextually generalisible nature.

Rather than expanding the overarching research objective, these two specific questions function as the empirical extension of the overarching research question. Together, they examine the empirical implications of the proposed reconceptualisation of privacy as a state developed in the proceeding theoretical examinations. By addressing these questions, the study empirically investigates what types of privacy states consumers perceive in the context of OBA, and addresses debates on the contextual nature of privacy. The following subsection discusses in greater detail the role of these research questions in guiding the empirical investigation.

7.3 Research Questions of the Empirical Study

In Chapter 2, it was established that the majority of OBA research defines consumer privacy as information privacy- that is, control over personal data, specifically regarding who gathers and disseminates data about consumers' online behaviour

under what circumstances (Baek & Morimoto, 2012; Bleier & Eisenbeiss, 2015; Gironda & Korgaonkar, 2018; Ham, 2017; Jung, 2017; Kim & Huh, 2017; Li, 2011). However, the critical examination of privacy conceptualisations presented in Chapter 4 reveals an important issue associated with this conceptualisation. Specifically, the privacy concern scales widely used in OBA research exhibit a problem of "conceptual redundancy".

As OBA literature heavily draws upon existing privacy conceptualisation scales (Baek & Morimoto, 2012; Dolnicar & Jordaan, 2007), many of them "conceptual redundancy" issue: that is, the inconsistency of privacy conceptualisations and measurement methods (see Chapters 2 and 4 for a detailed review). In particular, while OBA studies often define privacy in terms of control, their measurement tools fail to assess control directly. Instead, they measure consumers' psychological states, values, attitudes, and behavioural intentions.

As previously argued, values, attitudes, and behavioural intentions are not dimensions of privacy itself, but states. That is, the critical examination of privacy conceptualisation indicates that, within OBA, consumer privacy should be conceptualised as a state. Accordingly, to empirically examine the specific states consumers perceive within the OBA, this chapter asks the first research question:

Q1: What privacy states would consumers perceive in the context of OBA?

Another critical implication arising from privacy conceptualisation relates to the contextual nature of privacy. In particular, scholars have long debated whether privacy should be understood as context-specific or as context-generalisable when applying across different contexts. Scholars who advocate for the context-specific view argue that privacy is highly dependent on specific situational factors, ranging from external environmental aspects (e.g., the type or domain of the research construct, location, and rationale) to individual characteristics (e.g., demographics and culture), and thus varies accordingly (Mowday & Sutton, 1993; Smith et al., 2011). In contrast, the opposing perspective holds that privacy is context-generalisable, suggesting that the fundamental experience of privacy transcends particular contexts: if individuals perceive that their privacy has been violated either/both through appropriateness or/and distribution, they may perceive a privacy violation regardless of the specific setting (Nissenbaum, 2004). This division frames the core debate concerning the nature of privacy (Smith et al., 2011).

Whilst the context-specific nature of privacy has been widely acknowledged in the fields of digital marketing (Martin & Murphy, 2017) and information systems (Smith

et al., 2011), this thesis argues that the emergence of recent empirical findings challenge this assumption. Bol et al. (2018) reported no significant differences in consumer privacy concerns regarding OBA across online health, news, and commerce contexts. Moreover, Bleier and Eisenbeiss (2015) found that privacy concerns were not significantly influenced by different levels of OBA personalisation. These findings suggest that the context-specific nature of privacy concerns warrants reconsideration, as privacy may, in fact, exhibit a degree of generalisability across different digital environments, especially defining privacy as a state.

Revisiting the conceptualisation of privacy as a state (see Chapter 2) offers a potential lens through which the context-generalisable nature of privacy can be more comprehensively understood. Defining privacy as a state inherently embeds its context-generalisable nature. Within this framework, privacy as a state refers to an individual's state of mind, with types and levels that fluctuate across different privacy settings. Defining privacy in contexts, which responds to Laufer and Wolfe (1977) assertion that "privacy is strongly tied to or defined by the experience of given situations (p. 25)", thus forms the conceptual foundation supporting the notion that privacy embeds the context-generalisable nature.

Consider, for example, the OBA. Under the conceptualisation of privacy as a state, if consumers feel that advertisers' actions don't align with their expectations of norms in

OBA, such as by feeling intrusive (Bleier & Eisenbeiss, 2015), creepy (Phelan et al., 2016), or otherwise inappropriate, they would perceive their privacy as violated. Conversely, if consumers are comfortable with advertisers distributing their information in this manner, no privacy violation is perceived. Similarly, in interpersonal contexts such as marital relationships, which is the typical setting for the seminal Communication Privacy Management theory (Petronio, 1991), privacy judgments also occur, albeit in different forms. For instance, it may be common for one spouse to share private information with family members (Petronio, 1991); if the individual perceives such sharing as appropriate, no privacy violation is experienced. Conversely, if the individual feels a sense of "turbulence," a privacy violation is perceived.

Both examples illustrate that perceptions of privacy violations are rooted in individuals' subjective states of being violated, although the specific *types* and *intensities* of these states vary. Building on this observation, the thesis argues that contextual factors directly influence individuals' privacy states. What varies across contexts is not the existence of the privacy state itself, but rather the particular *types* and *intensities* through which that state is experienced. Framing privacy as a state, therefore, enables to capture the nuanced variations in individuals' perceptions of privacy across diverse contextual situations. By capturing these variations, this thesis proposes that privacy, conceptualised as a state, embraces a context-generalisable

nature. To further advance this theoretical proposition, the second research question is posed as follows:

Q2: Are the privacy states in OBA associated with other contexts?

7.4 Research Methods: A Mixed-Methods Research

To answer the above research questions, this study uses a mixed-methods approach with an exploratory sequential design (Creswell & Clark, 2017). An exploratory sequential design includes a qualitative phase followed by a quantitative phase. The following sections elaborate on each phase of the study, beginning with the qualitative sampling strategy, data collection procedures, and thematic analysis, followed by the quantitative phase, including survey design, statistical analyses, and integration of findings.

7.4.1 Mixed-Methods Research: An Exploratory Sequential Design

7.4.1.1 Mixed-Methods Research. A mixed-methods research was employed in the current study to answer the research questions. According to Johnson et al.'s (2007, p. 123) definition of the mixed methods (see below):

"*Mixed methods research is the type of research in which a researcher or team of researchers combines elements of qualitative and quantitative research approaches (e.g., use of qualitative and quantitative viewpoints, data collection, analysis, inference techniques) for the purposes of breadth and depth of understanding and corroboration. (p. 123)*"

As Creswell and Clark (2017) note, this definition frames mixed methods primarily as a methodology, which is a guiding rationale for conducting research. Building on this perspective, they offer a more comprehensive definition that highlights the core characteristics of mixed-methods research, as follows:

"*In mixed methods, the researcher*

- *collects and analyses both qualitative and quantitative data rigorously in response to research questions and hypotheses,*
- *integrates (or mixes or combines) the two forms of data and their results,*
- *organizes these procedures into specific research designs that provide the logic and procedures for conducting the study, and frames these procedures within theory and philosophy (p. 41).*"

Based on these definitions, it can be concluded that mixed-methods research is particularly appropriate for studies characterised by methodological, conceptual, or interpretative complexity or combination. The core strength of the mixed-methods lies in combining qualitative and quantitative approaches as this offers a more comprehensive understanding of a given phenomenon than either approach could achieve alone. As such, this method is highly suitable for studies that require both depth and breadth of understanding, that address complex or multi-layered research questions, and that involve high demands for interpretation, triangulation, or data corroboration, where findings from one method help to explain or validate those from the other (Creswell & Clark, 2017). As such, mixed methods research has been used in multiple research studies across different professional disciplines, including physical, financial, and political (Creswell & Clark, 2017).

In light of these characteristics, the current study adopts a mixed-methods design to address two interconnected research questions concerning the contextual and generalisable nature of privacy as a state. Specifically, Research Question 1 (RQ1) asks: What privacy states do consumers perceive in OBA? This exploratory question calls for an interpretive approach capable of capturing the affective, situational, and experiential dimensions of privacy as expressed by participants. To address this, the qualitative phase should be employed. In contrast, Research Question 2 (RQ2) asks: Are the privacy states in OBA generalisable across contexts? This is a confirmatory

question that requires systematic measurement across a broader sample to determine the consistency and variation of these descriptors across different national and situational contexts. This has been addressed through a quantitative phase. Most importantly, the integration of these two methodological strands not only allows for a deeper theoretical understanding of privacy as a state but also strengthens the empirical rigour of the findings by testing the conceptual output of the qualitative phase through cross-cultural generalisability. As such, the use of a mixed-methods approach is both theoretically justified and methodologically essential for achieving the aims of this study.

7.4.1.2 An Exploratory Sequential Design. Having established the rationale for employing a mixed-methods research design based on both the methodological strengths of combining qualitative and quantitative approaches and the specific demands of the research questions, researchers need to choose a suitable design rigorously (Creswell & Clark, 2017). When conducting a mixed-methods research, there are three main typologies of core mixed methods designs (see Table 5) for researchers to choose from: convergent design, explanatory sequential design, and exploratory sequential design (Creswell & Clark, 2017). These three designs differ from: (1) the intent of a design; and (2) the sequential ordering of the qualitative and quantitative phases.

The choice of a mixed-methods design should be guided primarily by the intent of the research questions. In the case of this study, both research questions aim to examine the extent to which the initial qualitative findings, regarding the experience of privacy as a state in the context of online behavioural advertising (OBA), can be generalised to other contexts. This clearly reflects an intent to both explore and generalise. As Creswell and Clark (2017) argue, the exploratory sequential design is particularly well-suited to such aims, as it involves first generating insights through qualitative research and then testing or generalising these findings with quantitative methods in a larger sample. This design has been successfully applied in previous studies exploring individuals' perceptions, for instance, perceptions of psychological distress among older, church-going African American men (Watkins et al., 2017) and perceptions of leadership among college students (Haber, 2012). Accordingly, the exploratory sequential design is the most appropriate methodological approach for this study, as it enables the exploration and generalisation of consumers' perceptions of privacy as a state across diverse contextual settings.

Table 5. *Three typologies of core mixed methods designs.*

Typologies	Intent of a design	Sequential ordering of the qualitative and quantitative phases
Convergent design	Converge: Converge results	The researcher implemented the quantitative and qualitative strands at the same time. the overall intent of the researcher is to converge or compare the results from the two databases.
Explanatory sequential design	Explain: Explain quantitative results	The researcher implemented the two strands in a sequence; the quantitative methods occurred first and had a greater emphasis in addressing the study's purpose, and the qualitative methods followed to help explain the quantitative results.
Exploratory sequential design	Explore: Explore and generalize findings	The researcher implemented the two strands in a sequence, the qualitative methods occurred first to explore a phenomenon and had a greater emphasis in addressing the study's purpose, and the quantitative methods followed to assess the extent to which the initial qualitative findings generalize to a population.

Note: This table summarises and adapts key concepts from Creswell and Clark (2017) regarding mixed methods research designs.

Figure 6 shows the procedural diagram for this exploratory sequential design. I began this exploratory sequential design by conducting an in-person semi-structured interview to explore the consumers' perceptions of privacy as a state in the context of OBA. Then, informed by the interview findings, I conducted an online survey of convenience participants from the US, China, and New Zealand to address the quantitative question. Finally, I interpreted the integrated results to assess which states identified in the interview were significantly associated with each context in the survey. The next sections explain how the two phases were employed and integrated to address the research questions.

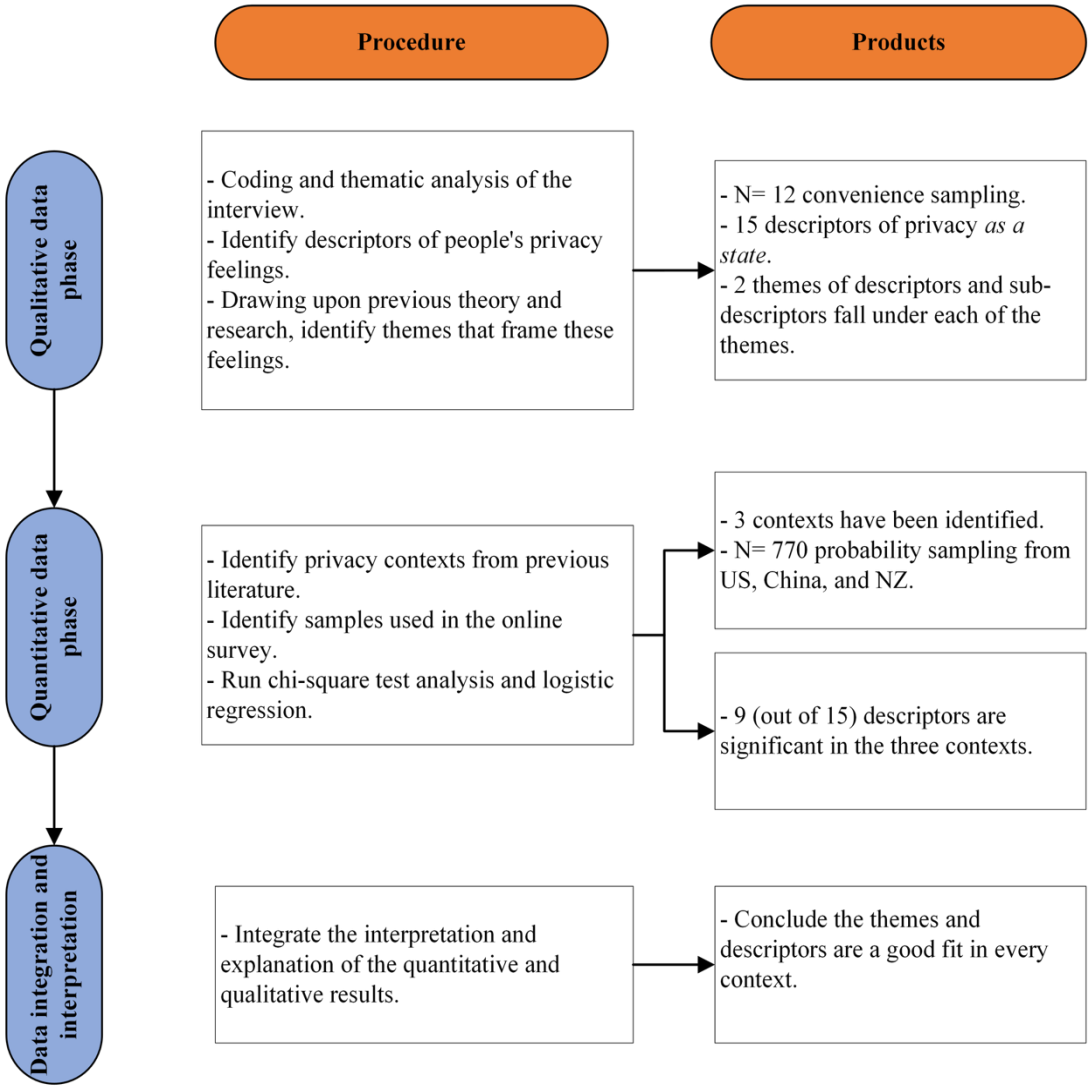


Figure 6. *Procedural Diagram for the Exploratory Sequential Design*

7.5 Qualitative Method: Semi-Structured Interview

7.5.1 Semi-Structured Interview

Semi-structured interview was chosen to address the objectives of this qualitative phase. The primary aim of the qualitative phase was to explore whether individuals experience privacy as a state in the context of online behavioural advertising (OBA), and if so, to understand how they cognitively and emotionally articulate such experiences.

Drawing on Bevan's (2014) work, interviews, particularly those with a phenomenological orientation, are recognised as effective tools for eliciting lived experience with reflective depth. Semi-structured interviews, in particular, strike a balance between structured guidance and open-ended exploration. Unlike fully structured interviews, which can constrain participant expression, or unstructured interviews, which may hinder cross-case comparison (Sekaran & Bougie, 2016), semi-structured formats allow for probing and participant-led elaboration. This makes them particularly well-suited for examining subjective, context-sensitive phenomena such as privacy (Busetto et al., 2020).

Moreover, the conceptualisation of privacy as a state presents additional methodological demands: it is an inherently internal, dynamic, and often implicit

experience that cannot be directly observed. The capacity of semi-structured interviews to accommodate depth, nuance, and reflexivity makes them particularly effective for identifying subtle indicators of such internal states (Busetto et al., 2020). This approach also facilitates the emergence of both descriptive language and contextual triggers that reveal how individuals situationally construct and experience privacy. Collectively, all the characteristics of semi-structured interviews align with the study's need to capture both the emergent descriptors of privacy states and the situational contexts in which those states are triggered.

7.5.2 Sampling

To ensure sufficient variation and depth while maintaining thematic saturation, the sample size followed the guidelines proposed by Malterud et al. (2016), who advocate for an information power approach to qualitative sampling. Furthermore, the participant recruitment strategy was informed by prior OBA-related qualitative studies (Phelan et al., 2016; Schaub et al., 2016; Ur et al., 2012; Yao et al., 2017), which have similarly relied on in-depth interviews to access individual attitudes, concerns, and responses to targeted advertising. In total, 12 participants were recruited for in-person interviews.

All participants were recruited through convenience sampling from the author's social networks in New Zealand via email invitations. Specifically, friends and colleagues within the university community were contacted directly to inquire about their willingness and availability to participate in an interview.

Table 6. *Characteristics of interviewees*

	N
Age range, years	
18-29	7
30-44	5
Education level	
Bachelor	1
Master	10
PhD	1
Nationalities	
Asian	8
Africa	1
USA	1
New Zealand	2

Table 6 presents the demographic characteristics of the interview participants. The sample consisted of 12 individuals, with the majority falling within the 18–29 age range (n = 7), followed by participants aged 30–44 (n = 5). In terms of education, the sample was predominantly highly educated, with 10 participants holding a Master's degree, one holding a PhD, and one holding a Bachelor's degree. This reflects a sample likely to possess advanced cognitive and reflective capacities, which is advantageous for engaging with abstract constructs such as privacy. Geographically, participants were originally from Asia (n = 8), with others from New Zealand (n = 2),

Africa (n = 1), and the United States (n = 1), offering a degree of cultural diversity relevant to the exploration of contextual privacy perceptions.

7.5.3 Procedure

To explore participants' contextual privacy perceptions in online behavioural advertising (OBA), a semi-structured interview protocol was designed and implemented. The offline interview process was divided into two stages: (1) procedures before the semi-structured interview, which established the ethical, procedural, and rapport-building groundwork; and (2) procedures within the interview itself, which involved an artificial scenario sharing followed by open-ended questions. Please refer to Appendix C for the semi-structured interview guide.

An initial email was sent to provide a brief introduction to the interview, including the interview topic, expected duration, and preferred format (online or in person) etc. During this initial email communication, participants were informed that an artificial video would be shown during the interview and were therefore encouraged to attend the interview in person. All participants agreed to this arrangement. Consequently, all interviews were conducted face-to-face.

Upon receiving participants' preliminary agreement, a follow-up email was sent to greet and thank them for their willingness to support my doctoral research and to confirm the interview schedule and format. Besides, they were also informed that the project had received ethical approval from Massey University's Human Ethics Committee (see Appendix A for the Massey Human Ethics Approval letter) and were requested to sign a Participant Consent Form (see Appendix B).

To create a smooth conversational atmosphere and save time for the interview, non-personal-identified rapport-building questions (see Table 7) were also posed in the email for them to fill out. This demographic context was later used to consider possible variations in privacy conceptualisation across demographic backgrounds.

Table 7. *Rapport-building questions*

Participants Information	
Age (or year of born)	
Gender	
Nationality	
Occupation	
Education level	
Living city and country	
How long have you been there?	

The second stage of the interview procedure, conducted in person, consisted of two structured phases: (1) a scenario-based simulation and (2) a set of open-ended interview questions with accompanying prompts and interventions.

To anchor participants' responses in a realistic and relatable experience, a controlled, artificial scenario was presented (see Appendix C for the article scenario). This staged scenario was carefully designed to trigger the appearance of an online behavioural advertisement based on prior browsing behaviour, thereby setting up the context for privacy-related reflection.

The artificial scenario was delivered off-line by screen-sharing a 5-minute video, unfolding in the following steps:

(1) Participants imagined they were considering buying a car and had heard positive comments about NISSAN. They searched "NISSAN" on Google.

(2) Upon landing on the official NISSAN New Zealand website, they navigated to the "100% Electric NISSAN LEAF" section to learn more due to rising fuel costs.

(3) They browsed details about the NISSAN LEAF, including visuals, specifications, and pricing.

(4) They exited the NISSAN website without making a purchase and then visited the Stuff News website to read the latest local news.

Participants were asked to imagine performing a set of common online searching and browsing tasks associated with car shopping, following the product context used in Aguirre et al.'s (2015) scenario development for online personalised advertising. Motor vehicles were selected as the focal product because they represent a high-involvement product category that typically requires extensive information search and online browsing during the purchase process (Dwivedi et al., 2021), making them a suitable product type for examining consumers' responses to personalised advertising.

Furthermore, as searching and browsing histories constitute common forms of online behavioural data used in OBA (Boerman et al., 2017), the scenario was designed around consumers searching for and browsing cars online to mimic a typical consumer journey that would lead to the display of an online behavioural advertisement. To enhance the realism of the scenario, the brand "NISSAN" was used, as the inclusion of an established and recognisable motor vehicle brand can facilitate participants' ability to imagine authentic consumption situations in digital advertising research.

Following the scenario, in the second phase of the in-person interview, participants were guided through six main open-ended interview questions:

1. Could you tell me whether you have noticed anything related to Nissan Leaf on the Stuff News website?

2. Could you please tell me what you do when you watch this ad? (Prompts) Why do you want to take this action?

3. Could you please tell me your feelings after watching this ad? Please describe to me your feelings. (Prompts) Do you think your privacy has been invaded by this ad? To what extent do you think this ad has invaded your privacy? You mentioned that you had a concern (were concerned/worried) for your privacy. Could you please describe what you mean by concern?

4. Have you ever seen this type of advertisement before? How much do you know about this advertisement?

(Intervention) Show [Material 1. What is OBA?].

Do you think you know more about this ad after watching the video? And how do you currently feel? Do you feel more or less [_____ (which you mentioned before)]? Besides this feeling, do you have other feelings?

5. How do you comment on this advertisement?/Do you think this advertisement is useful or not? What advantages and disadvantages does this commercial can offer you?

(Intervention) Show [Material 2. Benefits and Risks of OBA].

What would you like to do on this ad? What would you do in the future?

6. Is there anything else that you would like to comment on that I haven't already asked you about?

The first question served as a screening question, asking whether the participant had noticed anything related to the Nissan Leaf on the Stuff News website, which functioned to confirm their exposure to the behavioural advertisement. Participants who had not noticed any such content were shown the website again until they were exposed to the advertisement. The second question addressed behavioural intention, prompting participants to describe what actions they would take after seeing the advertisement and the reasons behind those actions. The third question explored participants' privacy state, inviting them to express their emotional responses to the ad and to articulate whether and how they felt their privacy had been invaded.

The fourth question elicited reflections on prior experience and knowledge, asking whether participants had encountered such advertisements before, how much they previously knew about them. An intervention was then incorporated in which participants were shown an existing educational video about online behavioural advertising (OBA). Following the video, participants were asked follow-up questions to assess whether the intervention influenced their understanding and, in particular, their emotional responses. The fifth question focused on perceived trade-offs, encouraging participants to evaluate the advertisement and reflect on its benefits and

risks. To facilitate this reflection, a list outlining the possible benefits and risks of OBA was presented to participants as an intervention. Participants were then asked about their behavioural responses in light of these considerations. Finally, the sixth question invited concluding remarks, giving participants the opportunity to share any additional thoughts not previously discussed during the interview.

7.5.4 Analysis

The interview data were analysed using manual thematic content analysis, a qualitative method that allows for breaking down a text into replicable, reliable, and valid themes by the use of explicit coding (Lambert, 2012). This method was chosen because it provides a flexible yet rigorous framework for capturing the complexity and subjectivity of participants' privacy experiences in response to online behavioural advertising (OBA). With only 12 participants and a narrowed focus of the interview, manually thematic analysis is practical. Most importantly, manual thematic analysis, as opposed to automated or software-assisted techniques, was particularly appropriate in this context due to the interpretive depth required to explore subtle emotional nuances and context-related meanings (Braun & Clarke, 2006).

The analytical procedure adopted in this study closely followed Braun and Clarke's (2006) six-phase process of thematic analysis, which is widely recognised as a flexible yet rigorous method for exploring qualitative data. The six phases include as follows:

Phase 1: familiarising yourself with your data - Phase 2: generating initial codes- Phase 3: searching for themes - Phase 4: reviewing themes - Phase 5: defining and naming themes - Phase 6: producing the report

This approach is particularly well-suited to research grounded in phenomenology, as it allows for a nuanced examination of participants' subjective experiences, while also acknowledging the active interpretive role of the researcher in meaning-making (Braun & Clarke, 2006).

Based on this logic, after transcribing and reading each interview multiple times, I began the analysis by immersing myself in the data through repeated readings of the interview transcripts in order to develop familiarity with the participants' narratives. Subsequently, I manually identified, isolated and coded each instance in which participants expressed a feeling, reaction, or evaluative judgement related to privacy within the OBA scenario. These expressions were highlighted directly within the

manuscript to ensure that their immediate context and discursive framing were preserved. I then extracted these expressions into a consolidated table, placed at the beginning of each participant's data file, alongside their demographic information, to facilitate subsequent review and comparison. This manual, iterative approach enabled close engagement with the data while maintaining the integrity, nuance, and tone of each participant's account. An example of the first page of one participant's file is provided in Appendix D.

Before identifying overarching themes, I first analysed all terms related to psychological states and excluded those that were not relevant to privacy. Subsequently, I applied the theoretical lens of dual-process theory (Kahneman & Tversky, 2013) to categorise the coded privacy-related descriptors into two thematic categories: intuitive feelings and reasoned feelings. These initial codes were manually applied to the data line by line to ensure the preservation of contextual and interpretive richness in participants' narratives. Particular attention was paid to emotionally charged language and its surrounding context to distinguish whether a descriptor represented an intuitive or a reasoned feeling. The coded states were then grouped according to semantic similarity and their theoretical alignment with Kahneman and Tversky's (2013) distinction between intuitive and deliberative processing. To illustrate how this distinction was applied in practice, I provide two representative coding examples below.

For example, the descriptor *uneasy* was coded as an intuitive feeling. Participants frequently used this term to describe an immediate affective reaction when encountering OBA, rather than a deliberative evaluation of privacy risks. As illustrated in the interview excerpts in Table 8, participants often expressed statements such as “I might feel uneasy about this ad” or “I have an uneasy sort of feeling,” which indicate a spontaneous emotional response triggered by the advertisement. Here, the descriptor was typically expressed as a direct feeling statement without an accompanying causal account of consequences, consistent with intuitive processing.

In contrast, the descriptor *concerned* was coded as a reasoning-based feeling. Unlike intuitive expressions that reflected immediate emotional reactions, participants’ use of *concerned* typically emerged from deliberative evaluations of potential risks and consequences associated with OBA. For instance, participants often articulated explicit reasoning processes, such as questioning the credibility of privacy protection claims (“I don’t think this is something that he’s going to be able to completely convince me… I still feel concerned”), comparing different types of advertisements (“I’m more concerned about political advertisements than commercial advertisements”), or reflecting on possible future risks related to data collection and misuse (“the internet has no borders, so my information could be collected by people who want to commit fraud”). These statements illustrate that the feeling of being

concerned was grounded in cognitive assessments of potential privacy threats rather than an immediate emotional reaction. This pattern aligns with reasoning processing in dual-process theory, where affect is reflected in explicit risk appraisal and causal reasoning.

7.5.5 Results

7.5.1.1 Descriptors.

Non-privacy-related descriptors. Initial coding of the transcripts revealed twenty affective descriptors used by participants to describe their feelings toward OBA and its perceived invasiveness (see Table 8). These included a wide array of emotions: creepy, afraid, scary, dangerous, risky, informative, threatened, offended, annoyed, embarrassed, uneasy, concerned, surprised, monitored, manipulated, violated, insecure, happy, dislike, and uncomfortable. However, upon a more nuanced review of the participants' explanations and contextual elaborations, five of these descriptors, namely surprised, informative, happy, uncomfortable, and embarrassed, appeared to be more closely linked to general user engagement with advertising or perceptions of utility rather than to the experience of privacy invasion per se. The following excerpts further illustrate how these specific descriptors were grounded in participants' lived experiences:

INFORMATIVE - Some participants framed OBA as functionally beneficial, especially when it delivered timely or relevant content. Participant 7 acknowledged a dual perception, stating that although there are “advantages and disadvantages,” receiving tailored product information during active browsing facilitated more contact with products of interest. Similarly, Participant 9 found ads “quite convenient,” particularly when they provided discounts or expanded shopping options. Echoing this sentiment, Participant 11 expressed appreciation for having relevant information “available,” suggesting that under certain circumstances, ads served as helpful extensions of their search behaviour. These reflections reveal a perception of utility that aligns OBA with convenience and efficiency, rather than evoking concerns about personal data use.

HAPPY - Positive emotional states were also reported, particularly when participants felt aligned with the ad content or its design. Participant 12 conveyed strong approval, noting, “I'll be absolutely happy with this.” The participant appreciated not only the relevance of the ad but also its delivery through a “user-friendly” platform that enabled them to “chase [their] own passion.” The sense of being recognised or valued by the company further enhanced their emotional response. Rather than reflecting a breach of privacy boundaries, such feelings point toward a sense of being understood or personally catered to, underscoring the commercial appeal of effective targeting.

UNCOMFORTABLE - In contrast, discomfort was a recurring theme, especially when ads were perceived as intrusive or mismatched with the participant's expectations or values. Participant 10 described a persisting sense of unease, particularly in response to political ads, noting that they "probably still feel uncomfortable" and that certain content heightened that discomfort. However, this discomfort was often framed in terms of content relevance or thematic mismatch, rather than a clear violation of privacy. This suggests that the unpleasantness stemmed more from the type of message than the mechanism by which it appeared.

SURPRISED - Surprise emerged as both an initial and fading reaction to ad targeting. Participant 3 reflected on this temporal shift, sharing that although they used to feel surprised by targeted ads, over time, it became routine: "I'm not surprised anymore." However, others still experienced surprise, often linked to the speed or accuracy of the targeting. Participant 4 described being "very surprised" when ads appeared "immediately" after a search, while Participant 10 noted that ads could still "pop up" and "catch [them] off guard." Despite these spontaneous reactions, surprise often denoted a reaction to efficiency or novelty, rather than a sense of surveillance or exposure, thus distinguishing it from core privacy concerns.

EMBARRASSED - Finally, embarrassment was reported when the visibility of targeted ads compromised participants' sense of privacy in social or shared digital

spaces. Participant 4 admitted to feeling “a little bit embarrassed” when others could see their ads, particularly if the content was private or sensitive. While this feeling suggests a boundary concern, it was socially rather than technologically rooted—related more to the interpersonal implications of ad visibility than to the algorithmic processes behind the ad’s placement. As such, embarrassment in these contexts reflected the situational awkwardness of shared environments rather than a subjective experience of privacy invasion.

Privacy-related descriptors. In contrast to feelings such as *informative* or *happy*, which were more closely linked to perceptions of ad utility or convenience, a deeper review of participants’ emotional descriptors, including *creepy, scary, offended, annoyed, uneasy, monitored, violated, dislike, afraid, dangerous, risky, threatened, concerned, manipulated,* and *insecure*, they reflect a nuanced range of privacy-related experiences. It is apparent that these feelings are not abstract or generalised reactions to advertising but are deeply rooted in participants’ perceptions of how their personal information is being accessed, used, and possibly exploited without consent. Drawing on Braun and Clarke’s (2006) reflexive thematic analysis, the decision to group the privacy-related emotional descriptors into seven distinct categories was based not solely on lexical similarity, but on the underlying emotional function, contextual meaning, and phenomenological depth expressed in participants’ narratives. This

nuanced grouping does not represent final thematic categories but is intended to aid the understanding and interpretation of the descriptors.

CREEPY / SCARY - For example, descriptors like *creepy* and *scary* frequently appeared when participants sensed that data collection practices were overly pervasive or invisible. Participant 1 described online tracking mechanisms as "*creepy crawlers*," suggesting a hidden, unsettling presence that captures user data across devices. Similarly, Participant 7 characterised the experience as "*very scary*," citing how the system appeared to know intimate details about their life, such as their location patterns and personal background. These expressions reveal that participants felt exposed in ways they neither authorised nor fully understood, highlighting a strong emotional response to the violation of informational boundaries.

OFFENDED/ANNOYED - The descriptor *offended* reflects a moral dimension in participants' reactions. For instance, Participant 6 explicitly stated feeling offended that the browser monitored their behaviour for ad targeting. This points to a sense of ethical breach, where the participant did not merely feel discomfort but felt wronged. Likewise, *annoyed* was commonly used to describe emotional fatigue and resistance in response to persistent advertising and repeated tracking. Participant 5's comment, "*It's so annoying, please don't trace me*," illustrates how a seemingly minor emotion

like annoyance becomes a privacy signal when linked to the experience of being continuously followed online.

UNEASY - The descriptor *uneasy* emerged when participants struggled to make sense of targeted ads or experienced emotional tension due to ambiguous or sensitive content. Participant 10 described an "*uneasy sort of feeling*" arising from how ads could "*influence decisions*." This subtle discomfort reflects an internal reaction to the erosion of decision-making autonomy and the uncertainty surrounding how much of one's behaviour is being observed.

MONITORED / VIOLATED / DISLIKE - A cluster of descriptors, *monitored, violated*, and *dislike*, articulated stronger, more sustained reactions to perceived surveillance. Participant 6 repeatedly used *monitored* to describe feeling watched, and even spied on, as a result of browsing-based targeting. The term *violated*, used by Participants 4 and 8, reflected a heightened emotional threshold. These participants did not feel neutral about targeting; otherwise, they felt their personal space and ideological beliefs were actively infringed upon. Similarly, *dislike* captured affective rejection, often rooted in the absence of consent and the perceived intrusiveness of cross-platform tracking.

AFRAID / DANGEROUS / RISKY / THREATENED - Descriptors like *afraid*, *dangerous*, *risky*, and *threatened* reflected more acute privacy anxieties. Participant 7 expressed fear of becoming a "target," and Participant 6 described a sense of being threatened by the real-time capture of their searches. *Dangerous* was invoked to communicate the perceived stakes of data exposure—such as the possibility that one's online activities could be exploited or traced in ways that compromise safety. The descriptor *risky*, as expressed by Participant 7, reflected behavioural adaptation; they deliberately withheld personal uploads online due to fears about data misuse. These terms reflect that privacy concerns were not only emotional but also behavioural and anticipatory, shaping how participants engaged with the digital environment.

CONCERNED - *Concerned* was used to express a lingering sense of unease, particularly when participants felt that platforms or advertisers might use their data for political or fraudulent purposes. For example, Participant 9 worried that political ads could lead others to infer group affiliations and target users accordingly. The concern here reflects both the complexity and the social consequences of privacy violations, not only does the individual feel at risk, but their identity and affiliations are also rendered vulnerable to external manipulation.

MANIPULATED / INSECURE - The descriptors *manipulated* and *insecure* capture a loss of agency and trust. Participant 3, who relied on ad blockers, explicitly used the

term *manipulated* to explain the benefit of avoiding targeted content, framing ads as intentional efforts to influence behaviour. Participant 6 described feeling *insecure* due to the lack of tools for anonymous browsing, expressing helplessness in protecting their privacy. These emotions link directly to autonomy and control, two foundational principles in privacy theory, and show that participants understood targeted advertising as more than a commercial mechanism; they viewed it as a psychological and behavioural intervention.

Collectively, these descriptors reflect how privacy is experienced not only as a matter of data flow or platform governance but as a heterophenomenological state. The participants' language reveals that their sense of privacy is emotionally charged, situationally triggered, and deeply embedded in their expectations of control, safety, and legitimacy. Rather than treating privacy as an abstract principle, these feelings provide evidence of how privacy violations are embodied and interpreted in OBA, confirming the relevance of privacy as a malleable experience.

Table 8. *Descriptors of privacy feelings and example expressions in the interview*

DESCRIPTORS	Example expressions
INFORMATIVE	Participant 7: but, if you need this thing at the moment, I browse this website, and then it provided me with a lot of, in this case, information, in fact, it is also easy for me to get more contact with this product. Anyway, there are advantages and disadvantages. Participant 9: sometimes when I'm looking at the ads, they give me some information, for example, discounts, and sometimes i find them quite convenient because they can give me more choices. Participant 11: so it's convenient to have information available to me.
HAPPY	Participant 12: I'll be absolutely happy with this. And I like it. Well, I can see not just the conflict made the company valued my interest. The platform also provide a user-friendly kind of platform for me to do any kind of chase. Let me use this word to chase my own passion and the company was able to kind of design the advert in such a way that it is intriguing.
UNCOMFORTABLE	Participant 10: I think I'd probably still feel uncomfortable. I feel like I'm getting trying to get a feel more uncomfortable when it was a political ad.
SURPRISED	Participant 3: I'm not surprised when I see an ad come up after I've been looking at a product. For example, recently, I was looking at buying cameras, and quite a lot of my ads have become camera based. And so I would imagine if I started to look for cars, all my ads would be different car manufacturers and car dealerships nearby. Participant 3: I used to be surprised, but nowadays it's just how it is, so I'm not surprised anymore. Participant 4: I was very surprised. They just immediately recommended the ads to me after I just finished searching. The whole process is too fast. Participant 10: Sometimes, something will pop up. Yeah, I'll be surprised, and it will catch me off guard.
EMBARRASSED	Participant 4: I would feel a little bit embarrassed, because, for example, when people use my computer, they will see the ads unintentionally when they pop up. I think I'm going to be more embarrassed if some private products are included in the ads.
CREEPY	Participant 1: I think it's something like the AI works there. There are creepy crawlers online. So I know that even if you are browsing a certain web page in another device, let's say, your cell phone, you're browsing something on cell phone, I do believe that it picks up your information.
SCARY	Participant 7: I think it's very scary, I would feel very scary, because he seems to have already got hold of most of my life, for example, the simplest, I think maybe they can locate me is an occasion that I usually go in and out of, and through the various things that I have exposed on the

	internet, and then it will also know my basic personal information, and then one of my occupations and so on, and I feel that I am very scared. Participant 9: I think it's a little bit uneasy and scary as well. You can easily be affected or controlled by those powerful people, and those adverts. So I will feel fearful.
OFFENDED	Participant 6: The browser directly monitors my behaviour and then targets me with ads, and I'm offended by that.
ANNOYED	Participant 3: Those things are quite annoying. And it's just, I guess that's less of being tracked but more of dealing with internet ads in general. Participant 5: It's so annoying, please don't trace me.
UNEASY	Participant 9: I might feel uneasy. I feel uneasy about this ad, and I feel more uneasy when facing more sensitive content. Participant 9: I think it's a little bit uneasy and scary as well. You can easily be affected or controlled by those powerful people, and those adverts. So I will feel fearful. Participant 9: And I might feel uneasy. But sometimes when I'm looking at the ads, they give me some information, for example, discounts, and sometimes I find them quite convenient because they can give me more choices. Participant 10: I have an uneasy sort of feeling, because it's keeping hold of sort of the data of what you're kind of looking at and can influence decisions in a way.
MONITORED	Participant 6: I feel like I'm being spied on, monitored, and threatened. I don't think it is a way of prediction, it's a monitoring. I would feel like the company is always staring at me. Participant 6: [when facing political ads] Even if I'm being monitored, I don't feel like I have anything to lose from that monitoring. Participant 9: I feel like my privacy is being monitored; my browsing history on these internet sites, is being monitored. I don't know how much he's monitoring. it's like he knows what I want, and then he can predict my mind and make me follow him.
VIOLATED	Participant 4: I might feel violated, but the degree wouldn't be very severe, 3 out of 10 degrees. If there were someone else present, my feeling of being violated is going to be slowly raised to 6 or 7 degrees out of 10. Participant 8: My feelings would be quite violated, because for example, what I search it's part of my ideology. Because they're trying to persuade me to vote for them because I already know what I want to vote for.
DISLIKE	Participant 5: I personally resent it. I don't like the idea of tracking what I was searching for and targeting me with ads tailored to these search histories on another website. Participant 6: But if it targets me on NZ Herald when I finish browsing Nissan's website, I'm going to resent it. Because I don't think it is a way of prediction, it's a monitoring. However, I will not resent the political ads as

	the commercial ads. While I know I'm being monitored, I don't feel that political ads can bring me immediate harm. Participant 6: If you continue targeting me with the same content, it will make me feel more disgusted.
AFRAID	Participant 7: I just feel very afraid of this thing. Participant 9: I think it's a little bit uneasy and scary as well. You can easily be affected or controlled by those powerful people, and those adverts. So I will feel fearful.
DANGEROUS	Participant 1: my contact details are endangered because, you know, they will be able to, to get my information and being able to associate it with the webpages that I'm interested in browsing. So I don't feel that safe when that when this happens. Participant 6: I feel that my browsing history has been stolen, and I do feel that browsing the web is very unsafe. Participant 7: I just feel like it's very dangerous. Because I would browse a lot in my daily life, we can't get away from life, can't get away from the internet.
RISKY	Participant 7: I usually won't upload too much, that is, some very personal information or photos, my family's information, because I feel that this I think it's risky.
THREATENED	Participant 6: I feel like I'm being spied on, monitored, and threatened. My day-to-day life, like what I search for and look at on the internet, will be immediately captured. Participant 7: I would feel that I will be taken as a target, my potential target I just feel like it could be a threat to my life.
CONCERNED	Participant 7: I just don't think this is something that he's going to be able to just completely convince me that this is 100% protection of my privacy, but I'm still going to feel a little bit concerned that even though it states that this is not going to be. Participant 8: I'm more concerned about political advertisements, instead of like commercial advertisements. Participant 9: I might think that the internet has no borders, so it's possible that my information could be collected by people who want to commit fraud. Although I haven't encountered it so far, I still doubt it and worry about my privacy. Participant 9: I feel okay with the commercial ads, but I will feel very concerned when it comes to political advertisements, which include advocating for you and so on. Because you cannot judge the facts, it is very easy to be led by their beliefs. I'm still worried about whether some people find out that you seem to belong to some group, and then they start contacting you because I believe they can track to your IP location, and your email address from your browsing history, and then they may send you a message to persuade you.

MANIPULATED	Participant 3: These software and browser extensions (ad blockers) that prevent ads being shown to me, so I can look at anything I want without being manipulated by people running ads through those platforms. Participant 8: I'm aware they're trying to manipulate me.
INSECURE	Participant 6: At the moment, I am not aware of any way to help me make my browsing trace-free. I would probably complain about these ads with my friends, telling them, “I'm very insecure about my online browsing lately.”

7.5.5.2 Themes of Intuitive Vs. Reasoning Feelings. Building on the previous section, which identified fifteen descriptors participants used to express their emotional responses to privacy invasion in the context of online behavioural advertising (OBA), this section further examines the nature of these feelings. Specifically, it applies the conceptual framework proposed by Phelan et al. (2016), which categorises privacy-related emotions into two types: intuitive and reasoning feelings. This dual-process model offers a useful lens to explore how individuals process privacy threats, whether their reactions are instinctive and emotionally charged, or reflective and analytically driven.

According to Phelan et al. (2016), intuitive feelings are characterised as “automatic, fast, and often emotionally charged,” relying on heuristics and affective associations without conscious control—such as the immediate sense that something feels creepy or offensive. In contrast, reasoning feelings are “slower, effortful, and may be governed by logic,” often involving explicit risk assessment, judgment, or deliberation—such as evaluating whether a data practice is risky, manipulative, or

justifiable in light of perceived benefits. This typology builds directly on Kahneman's (2011) conceptualisation of System 1 (fast, intuitive) and System 2 (slow, deliberative) thinking, which underlies much of contemporary dual-process theory in psychology and behavioural decision-making (Tversky & Kahneman, 1974).

Drawing on this framework and grounded in the example expressions collected during interviews, I categorised the fifteen privacy-related descriptors into two groups. Descriptors classified as intuitive feelings include: *creepy, scary, offended, annoyed, uneasy, monitored, violated,* and *dislike*. These feelings were typically described in response to immediate emotional reactions triggered during or right after viewing the ad. For instance, participants reported feeling *annoyed, creepy,* or *uneasy* without offering detailed justifications, suggesting that these responses were rapid, affectively charged, and driven by gut-level discomfort or a generalised sense of threat. Such reactions reflect what Phelan et al. (2016), drawing on Kahneman and Tversky's dual-process theory, describe as automatic and heuristic-based processing, which responses that arise spontaneously, without conscious deliberation or effort (Kahneman, 2011; Tversky & Kahneman, 1974).

For example, the descriptor *scary* emerged when Participant 7 described how OBA felt like it had "already got hold of most of my life," including personal habits and affiliations. Similarly, *monitored* was used by multiple participants, such as

Participant 6, who equated the ad tracking to being “spied on” and “threatened.” The descriptor *uneasy* reflected a more diffuse but persistent emotional discomfort, as noted by Participant 10: “I have an uneasy sort of feeling… it can influence decisions in a way.” These expressions were not just lexical repetitions, but also conceptually linked by their immediacy, lack of cognitive justification, and emotionally saturated tone, all of which typified intuitive responses.

The same process was applied for the theme of Reasoned Feelings, though the latter reflected more cognitively mediated and deliberate responses. The descriptors *afraid*, *dangerous, risky, threatened, concerned, manipulated,* and i*nsecure* were classified as reasoning feelings. These were associated with participants’ reflective evaluations about the implications of OBA for their privacy and autonomy. For example, Participant 9 expressed concern about being targeted by political ads due to the possibility of third-party actors inferring group affiliations and contacting users without consent. Similarly, Participant 6 described feeling *insecure* due to the lack of technological means to prevent personal data exposure. These expressions were typically accompanied by explanations of perceived risks, ethical boundaries, or expected consequences, suggesting a slower, more cognitively effortful process consistent with Phelan et al.’s (2016) description of reasoning feelings regarding privacy.

Phelan et al. further demonstrated that privacy experiences often begin with an intuitive reaction, which may then trigger a more deliberate, reasoned evaluation of the situation, such as assessing the trade-offs between personalised targeting and potential privacy risks. My findings reflect this two-stage pattern: many participants first articulated spontaneous feelings (e.g., *offended, annoyed*) and then expanded on these with more considered reflections on surveillance, manipulation, and data security.

For example, one participant (see Appendix D) initially responded to the targeted advertisement with an instinctive emotional reaction, describing it as *uneasy* and *unsure*, and later adding that such ads could feel *creepy*. These spontaneous descriptors reflect an immediate, gut-level discomfort. However, as the conversation progressed, the participant offered a more reasoned appraisal, noting that targeted ads can "influence decisions in a way," and that they felt *unsure* because "it's keeping hold of... the data of what you're kind of looking at." This shift from emotional unease to reflective evaluation became more explicit when political ads were introduced: the participant remarked feeling "more uncomfortable" and explained that these messages attempted to "convince [them] to make a decision towards a certain ideology... without even making [their] own decision."

The participant's evolving reflection extended beyond feelings and into behavioural responses. While initially stating they would "probably won't click" on such ads due to awareness of being targeted, they also acknowledged occasional curiosity-driven engagement, "sometimes something will pop up... and I will click on it just because I'm curious." Ultimately, regardless of what deliberate responses, their responses illustrate the two-stage privacy response pattern: an immediate, intuitive feeling such as discomfort or offence, followed by a more analytical stance that weighs the benefits and risks within the given context.

By distinguishing between intuitive and reasoning feelings, this categorisation not only supports the idea that privacy is experienced both affectively and cognitively as a state, but also reinforces Phelan et al.' (2016) dual-process framework regarding privacy.

7.6 Quantitative Method: Online Questionnaire

7.6.1 Online Questionnaire

To answer Research Question 2 (Are the privacy states in OBA associated with other contexts?) and test the generalisability of privacy-related states across different contexts, a quantitative online survey was conducted. The central aim of this stage was to assess whether the privacy states identified in the semi-structured interviews

within the context of online behavioural advertising (OBA) are also associated with other privacy-related contexts.

The online questionnaire method offers distinct advantages in terms of scalability, content validity, and statistical generalisability (Field, 2024; Sekaran & Bougie, 2016), making it suited to the exploration of whether and which emotional responses generalise across diverse contexts.

In the current questionnaire, there are three representative privacy contexts have been assessed. One of the privacy environments examined in this study is OBA, as consumer privacy issues within the OBA context constitute the core focus of this thesis. Beyond OBA, two additional contexts have been selected to assess the generalisability of the privacy-state descriptors: changing rooms (Hasenbush et al., 2019) and spouses relationships (Petronio, 1991). These three contexts are purposefully selected to represent digital, physical, and interpersonal privacy contexts, respectively. Furthermore, they are commonly associated with privacy concerns and correspond to Laufer and Wolfe's (1977) three dimensions of privacy: environmental (precisely the socio-physical element), self-ego, and interpersonal privacy, respectively.

7.6.2 Sampling

The survey employed a cross-national, probability sampling strategy using two established online research platforms: SurveyMonkey and Credamo. Data collection was initially conducted through SurveyMonkey due to its reputation as a well-known platform offering high-quality data and efficient participant recruitment (Hu et al., 2025). However, during the data collection process, it became evident that without purchasing a paid participant panel, most respondents recruited through the author's networks were located in China and New Zealand.

To ensure the inclusion of participants from the United States and to improve the cross-national balance of the sample, Credamo was subsequently used. Compared with SurveyMonkey, Credamo, though relatively new, was chosen for its affordability and its explicit focus on global data collection (Hu et al., 2025), with operations based in the United States.

Efforts were made to ensure diversity across cultural and demographic variables. The decision to adopt an international sample was grounded in prior research indicating that privacy expectations are shaped by cultural norms and digital infrastructures (Trepte et al., 2017). Including participants from multiple countries not only

strengthened the external validity of the findings but also helped reduce potential cultural bias in interpreting affective responses to online privacy scenarios.

Specifically, participants were recruited from China, the United States, and New Zealand to capture variation across different digital environments and cultural contexts, particularly between Western and Eastern societies. These countries represent distinct regulatory frameworks and cultural orientations toward privacy and data sharing, which have been discussed earlier as important factors influencing how individuals perceive and respond to online behavioural advertising.

From a practical perspective, these countries also represent active digital advertising markets. However, empirical research on online privacy perceptions remains heavily concentrated in the United States, with comparatively fewer studies examining consumers in China and New Zealand. Including participants from these contexts, therefore, helps broaden the geographical scope of the research. In addition, the author's professional and academic networks facilitated access to participants in these regions, providing feasible participant pools for cross-national data collection.

The study received ethical approval from Massey University's Human Ethics Committee (see Appendix E for the approval letter). A total of 770 valid responses

(incomplete questionnaires have been excluded) were collected from three culturally and digitally distinct countries: the United States (n = 172, 22.3%), China (n = 525, 68.2%), and New Zealand (n = 73, 9.5%).

Table 9 summarises the demographic overview of the participants, showing variation across age, gender, education, and country of residence. In terms of gender, females represented the largest proportion of respondents (47.9%, n = 369), followed by males (33.1%, n = 255), with 12.2% (n = 94) preferring not to disclose their gender. Gender data were available for 93.2% of the sample.

Age distribution was relatively broad. The largest age group was participants aged 30–44 (30.9%, n = 238), followed by those aged 45–60 (24.0%, n = 185) and under 18 (22.5%, n = 173). Fewer respondents were aged 18–29 (9.2%, n = 71) or above 60 (5.1%, n = 39). Age data were reported by 91.7% of participants.

In terms of educational background, respondents were notably diverse. A significant proportion had only completed school-level education (39.4%, n = 303), while others reported holding a Bachelor's degree (29.1%, n = 224), a Master's degree (7.8%, n = 60), or a PhD (7.7%, n = 59). A smaller group (6.8%, n = 52) had completed some

form of tertiary education that did not culminate in a full degree. Overall, 90.6% of participants provided education data.

Regarding geographic distribution, the sample was predominantly from China (68.2%, n = 525), followed by the United States (22.3%, n = 172) and New Zealand (9.5%, n = 73), reflecting the targeted recruitment strategy and intended cross-cultural coverage.

It is notable from Table 9 that a small proportion of responses were missing regarding gender, age group, and education level, resulting in missing data rates of 6.8%, 8.3%, and 9.4%, respectively. As these items involve personal and potentially sensitive information, participants were not required to respond to these items due to ethical considerations. Moreover, given that the missingness remained below the commonly accepted threshold of 10% (Schafer & Graham, 2002), and the variables were not central to the research questions, the missing data rates are reasonable and acceptable, no imputation was performed.

Table 9. *Characteristics of online survey participants*

	N	%	
GENDER			
Female	369	47.9	
Male	255	33.1	
Prefer not to say	94	12.2	
Total	718		93.2
Missing	52		6.8
AGE GROUP, YEARS			
Under 18	173	22.5	
18-29	71	9.2	
30-44	238	30.9	
45-60	185	24.0	
Above 60	39	5.1	
Total	706		91.7
Missing system	64		8.3
EDUCATION LEVEL			
School	303	39.4	
Tertiary	52	6.8	
Bachelor	224	29.1	
Master	60	7.8	
PhD	59	7.7	
Total	698		90.6
Missing system	72		9.4
REGIONS			
Us	172	22.3	
China	525	68.2	
NZ	73	9.5	
Total	770		100

7.6.3 Procedure

Participants were invited to complete a 15-minute anonymous online questionnaire hosted on the SurveyMonkey and Credamo platforms. The survey was designed to simulate three hypothetical yet realistic privacy-related scenarios: (1) encountering targeted advertising based on prior online activity (OBA), (2) being present in an open-plan public changing room, and (3) experiencing a breach of interpersonal confidentiality in a romantic relationship. These scenarios were selected to represent

three distinct types of privacy contexts—digital, physical, and relational—and were presented as short written vignettes (see Appendix F).

After reading each scenario, participants were asked to indicate how they would feel in that situation by selecting any number of emotional descriptors from a pre-defined list. This list consisted of 26 terms, including *creepy, angry, monitored,* and *violated*, which derived from the thematic analysis conducted during the qualitative interview phase. This approach ensured that the emotional response options were grounded in the prior phase (Creswell & Clark, 2017). In addition to the fixed list, participants could write in any additional feelings they experienced, allowing for more individualised and nuanced responses.

To enhance ecological validity (Aguinis & Bradley, 2014), each scenario was followed by one or more context-specific questions for the purpose of manipulation. For example, participants were asked about their awareness of tracking technologies in the OBA scenario, prior exposure to open-plan changing rooms, or current relationship status and duration in the interpersonal vignette.

Finally, participants were asked to provide basic demographic information, including gender, age, education level, nationality, and cultural identification. The survey

concluded with a short privacy orientation scale consisting of four items measured on a 7-point Likert scale (from 1 = “strongly disagree” to 7 = “strongly agree”), assessing the perceived importance of informational control and personal boundaries.

All data were collected anonymously, and participants were informed of their right to withdraw at any time. Ethical approval and a full participant information statement was provided at the beginning of the survey (see Appendix F).

7.6.4 Analysis

To examine how emotional privacy descriptors varied across the three contexts, a chi-square test and a logistic regression were employed. First, Pearson’s chi-square tests were used to determine whether the distribution of each descriptor (as a binary dependent variable) varied significantly across the three privacy contexts (independent variable) (Field, 2024). This test was chosen due to its suitability for nominal (categorical) data and its ability to assess the strength of association between two variables (Field, 2024). A significance threshold of $p < .05$ was applied, with results below this level indicating a statistically significant association between a particular feeling descriptor and the context in which it was reported.

To further investigate the descriptors identified as significantly associated across the three contexts, binary logistic regression was conducted. This method allowed for the examination of both the direction and strength of these associations (Field, 2024). In each model, the interpersonal context was used as the reference (baseline) category, with dummy variables created for the OBA (Online Behavioral Advertising) and Changing Room contexts. The dependent variable in each model was the presence or absence of a specific descriptor (e.g., *creepy, scary, uneasy*).

Additionally, demographic covariates, including age group, gender, region, and education level, were included to control for potential individual differences in the likelihood of reporting each descriptor. The logistic regression models provided odds ratios (Exp(B)), which quantify the likelihood of participants selecting each descriptor in the OBA and Changing Room contexts relative to the interpersonal context. This approach enabled a deeper understanding of which contexts are more likely to elicit stronger emotional responses and how demographic factors might influence these relationships.

7.6.5 Quantitative Results: Generalisable Privacy State

7.6.5.1 Frequencies. All the descriptors under both themes have been selected by the participants; however, they vary in frequency across different contexts. Table

10 provides the frequencies of the descriptors under themes across the three contexts. All the descriptors that emerged during the interviews are present in all three privacy contexts. In the context of OBA, the most prevalent descriptors were *creepy* (n=215), *monitored* (n=208), and *risky* (n=185). The least prevalent descriptors were *threatened* (n=50), *dangerous* (n=63), *violated* (n=66). In the context of changing room, the most prevalent descriptors were *uneasy* (n=152), *insecure* (n=150), *dislike* (n=147); the least prevalent descriptors were *manipulated* (n=21), *threatened* (n=44), *scary* (n=52). In the context of interpersonal relationship, the most prevalent descriptors were *dislike* (n=178), *offended* (n=153), *annoyed* (n=194); the least prevalent descriptors were *monitored* (n=21), *manipulated* (n=28), *dangerous* (n=36).

In summary, the OBA context tends to evoke stronger feelings of being *creepy*, *monitored*, and *risky*, which align with concerns about privacy invasion in online spaces. The changing room context generates more feelings of *uneasy* and *insecure*, likely due to the vulnerability associated with physical privacy concerns in such spaces. The interpersonal relationship context, meanwhile, elicits higher levels of being *offended*，*dislike*, and *annoyed*, possibly due to social interactions that may feel intrusive. Interestingly, the *monitored*, which has been chosen as the most prevalent descriptor in OBA, conversely becomes the least prevalent in the interpersonal

relationship. Due to the complexity of frequency across different contexts, it is important to note that further examination is necessary.

Table 10. *Frequencies of privacy descriptors across the three privacy contexts*

	OBA		**Changing Room**		**Interpersonal**	
	n= 770		n=770		n=770	
Descriptors	n	%	n	%	n	%
Creepy	**215**	27.9	**130**	16.9	**66**	8.6
Scary	**75**	9.7	**52**	6.8	**37**	4.8
Offended	**126**	16.4	**135**	17.5	**153**	19.9
Annoyed	**85**	11	**91**	11.8	**149**	19.4
Uneasy	**103**	13.4	**152**	19.7	**88**	11.4
Monitored	**208**	27	**75**	9.7	**21**	2.7
Violated	**66**	8.6	**57**	7.4	**78**	10.1
Dislike	**106**	13.8	**147**	19.1	**178**	23.1
Afraid	**102**	13.2	**124**	16.1	**95**	12.3
Dangerous	**63**	8.2	**61**	7.9	**36**	4.7
Risky	**185**	24	**91**	11.8	**61**	7.9
Threatened	**50**	6.5	**44**	5.7	**39**	5.1
Concerned	**98**	12.7	**82**	10.6	**105**	13.6
Manipulated	**110**	14.3	**21**	2.7	**28**	3.6
Insecure	**159**	20.6	**150**	19.5	**69**	9.0

Note: Percentages do not total 100 because responses could fall into more than one theme. Additionally, percentages were rounded.

7.6.5.2 Chi-Square Tests. Chi-square tests were conducted after computing frequency distributions to examine whether there are statistically significant associations between the reported feelings and the three privacy-related contexts:online behavioural advertising (OBA), changing rooms, and interpersonal relationships. While frequency tables provide a descriptive overview of how often each feeling descriptor was selected within each context, they do not indicate

whether these observed differences are statistically meaningful. The chi-square test is a non-parametric test particularly suited for categorical data (Field, 2024), such as feelings (e.g., *creepy, annoyed, monitored*) distributed across independent groups (i.e., the three contexts). Running chi-square tests enables a more rigorous analysis of whether the emotional responses vary by context beyond what would be expected by chance, thus helping to assess the contextual generalisibility of different privacy-related emotional states.

Table 11 summarises the results of the chi-square tests, which assess which feeling descriptors are significantly associated across three contexts. Based on their chi-square values and p-values, intuitive descriptors, including *offended (*$\chi^2 = 3.337$, $p = .189$*)* and *violated (*$\chi^2 = 3.629$, $p = .163$*)*, are not significantly different across contexts. As such, I cannot reject the null hypothesis, assuming that there is no association between people's feeling *offended* and *violated* across three contexts. However, *creepy* ($\chi^2 = 99.214$, $p < .001$), *scary* ($\chi^2 = 14.427$, $p < .001$), *annoyed* ($\chi^2 = 26.841$, $p < .001$), *uneasy* ($\chi^2 = 23.015$, $p < .001$), *monitored* ($\chi^2 = 210.513$, $p < .001$), and *dislike* ($\chi^2 = 22.323$, $p < .001$) show significant associations with the three contexts, suggesting that these intuitive feelings of privacy invasion are significantly associated with OBA, changing room and interpersonal relationship.

Notably, the especially high chi-square values of *creepy* ($\chi^2 = 99.214$) and *monitored* ($\chi^2 = 210.513$) indicate substantial variation: participants are significantly more likely to feel monitored and creeped out in certain contexts than others. Further testing is warranted to more rigorously examine this relationship.

Table 11. *Summary of chi-square tests between descriptors and three contexts*

	Contexts		
	OBA	C Room	Interpersonal
	χ2	df	Sig. (2-sided)
Intuitive theme			
Creepy**	99.214	2	<.001
Scary**	14.427	2	<.001
Offended	3.337	2	.189
Annoyed**	26.841	2	<.001
Uneasy**	23.015	2	<.001
Monitored**	210.513	2	<.001
Violated	3.629	2	.163
Dislike**	22.323	2	<.001
Reasoning theme			
Afraid	4.917	2	.083
Dangerous	9.119	2	.010
Risky**	87.244	2	<.001
Threatened	1.452	2	.484
Concerned	3.338	2	.188
Manipulated**	99.246	2	<.001
Insecure**	46.630	2	<.001

Turning to the reasoning descriptors, including *afraid* ($\chi^2 = 4.917$, $p = .083$), *dangerous* ($\chi^2 = 9.119$, $p = .010$), *threatened* ($\chi^2 = 1.452$, $p = .484$), and *concerned* ($\chi^2 = 3.338$, $p = .188$) show no significant relationship with the contexts. However, descriptors, including *risky* ($\chi^2 = 87.244$, $p < .001$), *manipulated* ($\chi^2 = 99.246$, p

< .001), and *insecure* ($\chi^2 = 46.630$, $p < .001$), are significantly associated with the contexts. Notably, the higher chi-square values of *risky* ($\chi^2 = 87.244$) and *manipulated* ($\chi^2 = 99.246$) suggest a very strong and significant association between the feeling of creepiness and the three contexts. This means that some contexts make people feel significantly riskier and more manipulated than others. Further testing is warranted to more rigorously examine this relationship.

7.6.5.3 Logistic Regression. Although the chi-square tests identified descriptors that varied significantly across the three contexts, it does not indicate the direction or strength of that relationship in each specific context. As such, a series of binary logistic regressions was conducted to further examine in which context each significant descriptor was most likely to be triggered (Full results and model coefficients for each descriptor can be found in Appendix G).

Binary logistic regression is particularly well-suited for this purpose as it models the probability of a binary outcome, in this case, whether or not a specific feeling descriptor was selected, based on categorical predictors (Field, 2024). It allows for the estimation of odds ratios that quantify the likelihood of an outcome occurring under different conditions (Field, 2024), making it a powerful tool for contextual comparisons in behavioural research (Menard, 2001).

While chi-square results revealed overall contextual differences, logistic regression enables a more fine-grained analysis by estimating the magnitude and direction of contextual effects, while controlling for individual-level covariates (i.e., age, region, gender, and education). This is critical for understanding not only whether, but how, specific feelings of privacy violation manifest differently across contexts.

That is, I conducted a series of binary logistic regression analyses (with each descriptor, e.g., feeling *creepy*, as the dependent variable, and context plus demographic covariates as predictors) to further examine which context evokes stronger emotional responses. In other words, beyond identifying descriptors that vary significantly across the three contexts, the aim here is to determine which specific context is more likely to trigger each emotional response. This allows for a deeper investigation into how contextual differences influence the likelihood of experiencing particular privacy-related emotions. For example, in which context are participants more likely to feel *creepy*? And is this likelihood moderated by individual-level factors such as education, gender, region, or age, and if so, how do these variables shape the relationship?

For each descriptor (dependent variable coded as 1 = feeling present, 0 = not present), the predictor variable was context (reference = interpersonal), with demographic covariates entered simultaneously. The results indicate distinct patterns across the "intuitive" and "reasoning" descriptors. Please refer to Table 12 for an overview of the logistic regression for all descriptors.

Among the intuitive descriptors, participants were significantly less likely to feel *creepy* in both OBA and CR contexts compared to interpersonal ones, with the odds ratios of 0.45 in OBA and 0.20 in CR. This means participants were 55% less likely in OBA and 80% less likely in CR. A consistent pattern was found for *scary* and *monitored*, both of which were considerably more likely to be reported in interpersonal contexts. In contrast, *uneasy* was more likely to be triggered by OBA than by interpersonal scenario, while the CR context did not show a significant difference. For *annoyed*, the CR context was a significantly stronger trigger than both interpersonal and OBA settings, while no significant difference was observed for OBA. Finally, *dislike* was more likely in both mediated contexts as well, with the effect particularly pronounced in the CR scenario.

Among the reasoning-based descriptors, *risky* was significantly more likely to be reported in interpersonal settings than in OBA and CR, with the odds of reporting being 60% and 75% lower in the latter two, respectively. *Insecure* was more likely to

be triggered by the interpersonal scenario, while the OBA context did not show a significant difference. The descriptor *manipulated* was far less likely to be reported in OBA or CR contexts. This may suggest that the feeling of being *manipulated* is most often associated with close interpersonal settings, possibly due to the relational expectations embedded in face-to-face interactions.

Across models, several demographic variables exerted significant effects. For example, younger participants (particularly those aged 18-29) were more likely to report feelings such as *uneasy*, *annoyed*, and *insecure*, while participants from China or the US consistently showed lower likelihood of reporting negative feelings compared to those from New Zealand. Additionally, educational attainment showed some differentiated effects, particularly in the case of *scary* and *uneasy*, where participants with postgraduate degrees were more likely to report negative emotions. Gender effects were modest overall but notable in feelings such as *manipulated* and *monitored*, where male participants were significantly more likely than others to report such feelings.

Together, these logistic regression models illuminate the contextual specificity of privacy-related emotional responses and reveal how background characteristics may amplify or mitigate these feelings.

Table 12. *Full logistic regression summary for descriptors across contexts*

Note: Reference category = Interpersonal context; OR < 1 indicates a lower likelihood of experiencing the descriptor. Model χ^2 = omnibus test of model fit; Nagelkerke R^2 = pseudo R^2 indicating variance explained.

Descriptor	Context Comparison	B	SE	OR	95% CI for OR	p	Model χ^2 (df)	Nagelkerke R^2	Significant Demographics
Creepy	OBA vs Interpersonal	-0.793	0.142	0.452	[0.343, 0.597]	<.001	278.60 (14)	0.207	Age, Region, Education
	CR vs Interpersonal	-1.607	0.169	0.200	[0.144, 0.279]	<.001			
Scary	OBA vs Interpersonal	-0.425	0.203	0.654	[0.439, 0.974]	.036	108.18 (14)	0.125	Age, Region, Education
	CR vs Interpersonal	-0.780	0.222	0.459	[0.297, 0.708]	<.001			
Annoyed	OBA vs Interpersonal	0.138	0.175	1.148	[0.814, 1.618]	.431	288.76 (14)	0.228	Age, Region
	CR vs Interpersonal	0.753	0.165	2.124	[1.538, 2.933]	<.001			
Uneasy	OBA vs Interpersonal	0.592	0.152	1.808	[1.343, 2.435]	<.001	148.56 (14)	0.120	Age, Region, Education
	CR vs Interpersonal	-0.112	0.167	0.894	[0.645, 1.241]	.504			
Monitored	OBA vs Interpersonal	-1.275	0.157	0.279	[0.205, 0.380]	<.001	226.75 (14)	0.193	Region, Gender
	CR vs Interpersonal	-2.553	0.244	0.078	[0.048, 0.126]	<.001			
Dislike	OBA vs Interpersonal	0.361	0.147	1.434	[1.076, 1.911]	.014	54.58 (14)	0.042	Gender
	CR vs Interpersonal	0.600	0.142	1.822	[1.378, 2.409]	<.001			
Risky	OBA vs Interpersonal	-0.916	0.151	0.400	[0.298, 0.538]	<.001	127.73 (14)	0.107	Age, Region, Gender, Education
	CR vs Interpersonal	-1.401	0.172	0.246	[0.176, 0.345]	<.001			
Manipulated	OBA vs Interpersonal	-1.919	0.265	0.147	[0.087, 0.247]	<.001	134.64 (14)	0.159	Region, Gender, Education
	CR vs Interpersonal	-1.575	0.233	0.207	[0.131, 0.327]	<.001			
Insecure	OBA vs Interpersonal	-0.064	0.135	0.938	[0.720, 1.222]	.637	75.63 (14)	0.061	Age, Gender
	CR vs Interpersonal	-0.979	0.163	0.376	[0.273, 0.517]	<.001			

7.7 Integration of Qualitative and Quantitative Findings

The integration of qualitative and quantitative strands is the key point of convergence in this exploratory sequential mixed-methods study. This section draws together findings from the semi-structured interviews and the online survey to examine how privacy-related feelings, which are conceptualised as descriptors of privacy as a state, manifest both experientially and statistically across different privacy contexts. The integration was achieved through a joint data display (see Table 13), which aligns qualitative themes with quantitative statistical tests to provide a cohesive interpretation of the results.

In the qualitative phase, 15 unique descriptors were extracted from participant narratives in the OBA context. These descriptors were grounded in participants' real-time or reflective reactions to perceived privacy invasions. Based on their content and emotional tone, the descriptors were categorised into two overarching themes: intuitive feelings, which are spontaneous, affective reactions (e.g., *creepy, uneasy, monitored)*, and reasoning-based feelings, which are cognitively appraised and evaluative (e.g., *risky, manipulated, insecure*). This classification reflects dual-process theories of decision-making and emotion, which distinguish between automatic (System 1) and reflective (System 2) psychological responses.

In the quantitative phase, the survey tested whether these privacy descriptors were applicable and significantly associated with three different contexts: online behavioural advertising (OBA), changing rooms (physical privacy), and interpersonal relationships (social privacy). The aim was not only to determine the statistical relevance of these descriptors across contexts but also to assess whether feelings identified in the OBA context could be generalised to other privacy-related situations. The statistical tests, including chi-square analyses and logistic regressions, enabled identification of descriptors that had strong, moderate, or negligible contextual associations.

Six out of eight intuitive descriptors, including *creepy, scary, annoyed, uneasy, monitored,* and *dislike*, were found to be significantly associated with context ($p < .001$), indicating that feelings within this category are highly context-sensitive. These results suggest that intuitive feelings, while spontaneous, are not uniform across situations; rather, they are shaped by the perceived nature and severity of the privacy breach. Descriptors such as *offended* and *violated*, although salient in qualitative accounts, did not differ significantly across contexts, possibly indicating a more stable, baseline reaction to privacy invasion that transcends specific environments.

For the reasoning-based descriptors, three out of seven (e.g. *risky*, *manipulated*, and *insecure*) also demonstrated statistically significant contextual variation. These findings confirm that even evaluative, reflective assessments of privacy can vary with context, challenging assumptions that such feelings are static or exclusively shaped by individual traits.

The joint data display consolidates these findings, mapping the descriptors that were both qualitatively emergent and quantitatively significant. This integration underscores several key insights: (1) Some descriptors (e.g., *creepy, monitored, risky*) are not only frequent but also strongly associated with specific contexts, suggesting they are core features of privacy as a state. (2) Others (e.g., *threatened, concerned*) are less sensitive to contextual variation, suggesting a background-level awareness or expectation of privacy, regardless of the situation.

In summary, this integration phase demonstrates that feelings related to privacy are simultaneously subjective and statistically generalisable, reinforcing the idea of privacy as a heterophenomenological state. By uniting experiential depth with empirical breadth, this mixed-methods study lays the foundation for theorising privacy states as contextually dynamic and psychologically nuanced.

Table 13. *Privacy descriptors joint data display of qualitative and quantitative findings*

Qualitative themes	Quantitative tests		Mixed methods interpretation
Intuitive theme	Sig.	$\chi 2$	
Creepy	<.001	99.214	**Creepy**: Not only did it emerge (QUAL) as feelings of privacy invasion in OBA, but it was also found to be statistically significant (QUAN) in the contexts of OBA, changing rooms, and interpersonal relationships. Also, a very strong and significant association between feeling creepy and three contexts was found.
Scary	<.001	14.427	**Scary**: Not only did it emerge (QUAL) as feelings of privacy invasion in OBA, but it was also found to be statistically significant (QUAN) in the contexts of OBA, changing rooms, and interpersonal relationships. Also, a small and significant association between feeling scary and three contexts was found.
Offended	.189	-	**Offended**: Although it emerged (QUAL) as feelings of privacy invasion in OBA, it was not found to be statistically significant (QUAN) in the contexts of OBA, changing rooms, and interpersonal relationships.
Annoyed	<.001	26.841	**Annoyed**: Not only did it emerge (QUAL) as feelings of privacy invasion in OBA, but it was also found to be statistically significant (QUAN) in the contexts of OBA, changing rooms, and interpersonal relationships. Also, a moderate and significant association between feeling annoyed and three contexts was found.
Uneasy	<.001	23.015	**Uneasy**: Not only did it emerge (QUAL) as feelings of privacy invasion in OBA, but it was also found to be statistically significant (QUAN) in the contexts of OBA, changing rooms, and interpersonal relationships. Also, a moderate and significant association between feeling uneasy and three contexts was found.
Monitored	<.001	210.513	**Monitored**: Not only did it emerge (QUAL) as feelings of privacy invasion in OBA, but it was also found to be statistically significant (QUAN) in the contexts of OBA, changing rooms, and interpersonal relationships. Also, a very strong and significant association between feeling monitored and three contexts was found.
Violated	.163	-	**Violated**: Although it emerged (QUAL) as feelings of privacy invasion in OBA, it was not found to be statistically significant (QUAN) in the contexts of OBA, changing rooms, and interpersonal relationships.
Dislike	<.001	22.323	**Dislike**: Not only did it emerge (QUAL) as feelings of privacy invasion in OBA, but it was also found to be statistically significant (QUAN) in the contexts of OBA, changing rooms, and interpersonal relationships. Also, a moderate and significant association between feeling dislike and three contexts was found.
Reasoning theme			
Afraid	.083	-	**Afraid**: Although it emerged (QUAL) as feelings of privacy invasion in OBA, it was not found to be

			statistically significant (QUAN) in the contexts of OBA, changing rooms, and interpersonal relationships.
Dangerous	.010	-	**Dangerous**: Although it emerged (QUAL) as feelings of privacy invasion in OBA, it was not found to be statistically significant (QUAN) in the contexts of OBA, changing rooms, and interpersonal relationships.
Risky	<.001	87.244	**Risky**: Not only did it emerge (QUAL) as feelings of privacy invasion in OBA, but it was also found to be statistically significant (QUAN) in the contexts of OBA, changing rooms, and interpersonal relationships. Also, a very strong and significant association between feeling risky and three contexts was found.
Threatened	.484	-	**Threatened**: Although it emerged (QUAL) as feelings of privacy invasion in OBA, it was not found to be statistically significant (QUAN) in the contexts of OBA, changing rooms, and interpersonal relationships.
Concerned	.188	-	**Concerned**: Although it emerged (QUAL) as feelings of privacy invasion in OBA, it was not found to be statistically significant (QUAN) in the contexts of OBA, changing rooms, and interpersonal relationships.
Manipulated	<.001	99.246	**Manipulated**: Not only did it emerge (QUAL) as feelings of privacy invasion in OBA, but it was also found to be statistically significant (QUAN) in the contexts of OBA, changing rooms, and interpersonal relationships. Also, a very strong and significant association between feeling manipulated and three contexts was found.
Insecure	<.001	46.630	**Insecure**: Not only did it emerge (QUAL) as feelings of privacy invasion in OBA, but it was also found to be statistically significant (QUAN) in the contexts of OBA, changing rooms, and interpersonal relationships. Also, a moderate and significant association between feeling insecure and three contexts was found.

7.8 Discussion

This mixed-methods study makes a novel contribution to the conceptualisation of privacy by framing it as a heterophenomenological state—a construct that captures both the lived, subjective experience of privacy and the measurable, generalisable patterns of privacy-related feelings across contexts. The research design adopted an exploratory sequential approach to address two core questions:

RQ1: What privacy states would consumers perceive in the context of OBA?

The findings affirm that privacy violations are experienced and felt through various state-related feelings. The qualitative interviews revealed a rich set of descriptors, ranging from *creepy, scary,* and *monitored* to *risky, manipulated,* and *insecure*, that reflect both immediate affective reactions and more reasoned evaluations of privacy-related harm. These descriptors confirm that privacy is experienced not just as control but also through affective states that often precede conscious reasoning.

Furthermore, by categorising descriptors into intuitive and reasoning themes, the study draws attention to the dual-process nature of privacy state. This distinction aligns with existing models of decision-making in psychology and consumer behaviour, where both fast, automatic reactions and slow, deliberate appraisals inform responses to external stimuli. Applied to the domain of privacy, this suggests that consumers' perceptions of OBA do not stem solely from logical analysis of data use, but also from intuitive and reasoned feelings of being watched, exploited, or exposed.

RQ2: Are the privacy states in OBA generalisable across contexts?

The quantitative findings confirm that several privacy states initially identified in the context of online behavioural advertising (OBA) can, to a significant extent, be generalised to other contexts, although this requires further large-scale validation.

Chi-square and logistic regression analyses revealed that certain emotional responses, particularly feelings of being *creepy*, *monitored*, *risky*, and *manipulated*, consistently align with perceived privacy violations across all three contexts examined. This provides robust empirical support for the proposition that privacy experiences are trans-contextual, reinforcing the view that privacy as a state is shaped by context but can also transcend specific situations.

In contrast, feelings such as *offended*, *concerned*, *threatened*, or *violated*, although frequently reported, did not show statistically significant variation across contexts. This suggests that these emotions may represent more generalised background responses, which is emotionally salient yet insufficiently sensitive to contextual distinctions. Consequently, their utility in capturing the dynamic, situational nature of privacy states may be limited, reducing their generalisability across diverse settings.

This variation is critical. It aligns with the definition proposed in this thesis, which conceptualises privacy states as malleable, occupying a continuum between no privacy and full privacy. Viewing privacy as a *state* enables the capture of this fluidity: individuals can shift from state types and mild discomfort to acute distress depending on contextual factors, the degree of perceived control, and the interpreted intentions of others.

Taken together, these findings provide strong support for a state-based reconceptualisation of privacy, one that is grounded in emotionally embedded experiences that can be generalised across contexts. The evidence suggests that when privacy is understood as a state, it is inherently variable and highly sensitive to individuals' interpretations of situational cues and perceived violations. What changes across contexts is not the existence of the privacy state itself, but rather the specific *types* and *intensities* of those states.

Moreover, the integration of qualitative depth with quantitative generalisability enhances the credibility of this conceptual shift. The convergence of phenomenological insight (as self-described in participants' own words) with statistically significant patterns (demonstrated through empirical testing) strengthens the construct validity of the conceptualisation. This dual confirmation not only legitimises privacy as a state-based construct but also provides a solid empirical and theoretical foundation for future research and theorisation in this area.

7.9 Contributions

This study makes several important contributions to the evolving literature on individual privacy, particularly within the context of Online Behavioural Advertising

(OBA). Theoretically, empirically, and methodologically, the research advances our understanding of privacy not merely as a right or control mechanism but as a lived, psychological state.

A central contribution of this study lies in its challenge to dominant conceptualisations of privacy that equate it primarily with control, right, or commodity. Instead, it reconceptualises privacy as a state: an heterophenomenological mind that people could self-describe and constitute from individuals' intuitive and reasoning responses to situational stimuli. Drawing on heterophenomenology (Dennett, 2003), the thesis introduces and operationalises the notion of privacy as a heterophenomenological state, meaning that privacy is best understood through the subjective expressions of those experiencing it. This perspective captures the layered, often non-rational, and emotionally rich nature of privacy states as they are perceived in real-life scenarios.

Furthermore, the study provides evidence that certain privacy-related emotional responses are generalisable across distinct settings involving varying degrees of personal data exposure and social sensitivity. While the experience of privacy is contextually shaped, consistent emotional responses, particularly intuitive descriptors such as *creepy, annoyed*, and *monitored*, and reasoning-based descriptors such as *risky*, *manipulated*, and *insecure*, were repeatedly observed across three diverse contexts: online advertising, physical changing rooms, and interpersonal information

sharing. This challenges the absolutist view that privacy experiences are entirely context-dependent and supports a more nuanced position that incorporates both contextual integrity and trans-contextual affective generalisability.

Methodologically, this study extends the application of an exploratory sequential mixed-methods design to the relatively underexplored domain of consumer privacy states. As discussed in Section 7.4.1, mixed-methods research has been widely applied across various professional disciplines, including the physical sciences, finance, and political science (Creswell & Clark, 2017). However, the exploratory sequential design, in particular, is often applied in exploring individuals' perceptions of psychological distress (Watkins et al., 2017) and perceptions of leadership (Haber, 2012). Its application in consumer privacy research, particularly to investigate privacy perceptions of states, remains scarce. This study, therefore, represents a pioneering effort to use mixed-methods in the domain of consumer privacy perceptions.

The initial qualitative phase explored rich, phenomenological data grounded in participants' experiences of privacy states, enabling the identification of emotional and cognitive responses to privacy violations. These qualitative insights were subsequently operationalised and tested through a large-scale quantitative survey across three representative privacy-involved contexts. This rigorous integration of qualitative and quantitative strands enhances the validity and generalisability of the

findings. As such, by demonstrating the empirical rigour and theoretical utility of the exploratory sequential design in the area of consumer privacy perceptions, the study does more than solve its specific research questions it also expands the boundaries of what mixed-methods research can achieve. In doing so, it provides a replicable methodological model for future privacy scholarship and makes a meaningful contribution to the broader evolution of mixed-methods research as a rigorous and epistemological strategy which covers the depth and breadth of a research topic (Watkins et al., 2017).

Finally, the findings carry several implications for marketing practitioners, platform designers, and policymakers. Reframing privacy as a psychological and emotional state highlights the importance of respecting the perceptual boundaries of individuals, not merely their legal rights or perceived control. For marketers, understanding that certain advertisements evoke feelings of manipulation or annoyed can inform more ethically grounded advertising strategies. For policy designers, recognising the generalisable nature of certain emotional responses can guide the development of user-centred data governance frameworks that account for emotional harm, not just informational risk. This approach substantively addresses consumers' emotional and psychological well-being, while contributing to a broader conceptual paradigm shift—from treating "privacy as control" as a measurable scholarly paradigms, to recognising "privacy as a state" as an individual shift (Hull, 2015; Smith et al., 2011).

7.10 Limitations and Further Research Recommendations

Despite its conceptual and methodological contributions, this study is subject to several limitations that should be acknowledged and addressed in future research. These limitations also present opportunities to extend and deepen the exploration of privacy as a state.

First, the sample size for the qualitative phase (12 participants) while relatively small, is adequate for phenomenological research (Bevan, 2014). Moreover, their educational levels focus on postgraduate qualifications, omitting individuals who hold only undergraduate degrees or lower. Consequently, future studies could increase the sample size and include a broader range of educational backgrounds to capture a wider variety of perspectives.

Additionally, as the quantitative phase included participants from multiple cultural contexts (the US, China, and New Zealand), future studies could benefit from a deeper exploration of cultural differences in privacy states. For instance, different cultural norms regarding privacy may influence the intensity and type of privacy states experienced in various contexts.

The study's quantitative findings reveal a notable difference in the number of generalisable intuitive descriptors and reasoning descriptors. Specifically, a greater number of intuitive descriptors were found to be significantly associated with all three contexts, while only three reasoning descriptors demonstrated significant associations. Therefore, future research can leverage this distinction to explore why individuals express more intuitive feelings in private settings and examine the specific connection between these intuitive feelings and reasoning-based feelings.

The findings on intuitive and reasoning descriptors contribute significantly to the further development of a robust measurement of privacy as a state. The tested descriptors show significant associations across various contexts, which should be included in privacy state measurements to reflect how individuals perceive privacy invasions. As such, I encourage further research to develop a privacy state measurement scale.

7.11 Conclusion and Implications

This mixed-methods study provides empirical support for the core argument of this thesis, namely, that privacy is best conceptualised as a heterophenomenological state, rather than a static condition or binary status. The qualitative phase revealed how individuals intuitively and cognitively respond to perceived privacy invasions across

varying contexts, highlighting the emotional richness and situational triggers embedded in privacy experiences. Through in-depth interviews, participants articulated both implicit, affective reactions (e.g., *creepy, uneasy, violated*) and reflective, evaluative responses (e.g., *manipulated, risky, insecure*) to targeted advertising practices, thus supporting the idea that privacy is felt, interpreted, and contextually constructed.

Building upon these insights, the subsequent quantitative phase enabled a broader generalisation of these privacy-related emotional states. The findings demonstrate that while the intensity and expression of privacy states are shaped by context, several descriptors, such as *creepy, annoyed, monitored, risky, manipulated, and insecure*, consistently emerged across multiple privacy-sensitive situations, including online behavioural advertising (OBA), changing room surveillance, and interpersonal disclosure. These generalisable affective markers lend empirical credibility to the conceptual model of privacy as a state, and confirm that certain privacy responses transcend specific environments, suggesting a deeper structure of contextual privacy dynamics.

Although the primary aim of this thesis is conceptual and theoretical in nature, the integration of empirical methods has strengthened the validity and applicability of the proposed shift toward a “privacy as a state” argument. With the conclusion of the

empirical component, the thesis finishes its relevant justifications regard privacy definition, indicating that the thesis now moves forward to address new theoretical problems.

The next chapter opens a new line of theoretical model development based on the findings of this empirical research and the critical examinations previously. The argument surrounding privacy as a heterophenomenological state will be reintroduced and substantially developed in Chapter 8, where it serves as the foundation for the formulation of the Contextual Privacy State (CPS) model.

Chapter 8: Development of Contextual Privacy State Model

8.1 Introduction

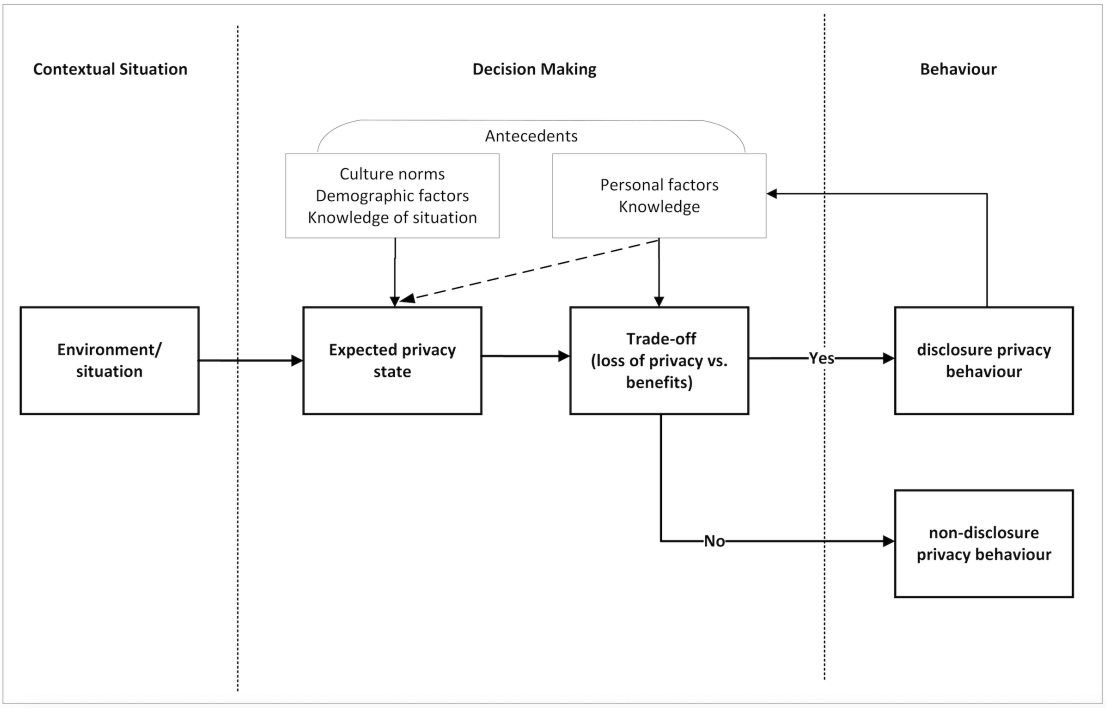
Critical examinations of previous privacy conceptualisations (Chapter 4), empirical studies (Chapter 5), and theoretical privacy models (Chapter 6) together reveal that many of these approaches used by OBA literature fall short in capturing the full and accurate picture of consumer privacy within the context of online behavioural advertising (OBA). This suggests that much of the existing academic output on privacy in OBA is lacking in cognitive success; that is, it fails to offer accurate and meaningful representations of the private phenomena it seeks to explain (Niiniluoto, 1999).

Based on the positive and negative results of critical examinations, this chapter introduces the Contextual Privacy State (CPS) model, a cognitively successful framework that more fully and effectively reflects the reality of consumer privacy within OBA. The CPS model is informed by insights from three foundational domains: (1) the conceptualisation of privacy, (2) empirical findings on privacy in OBA, and (3) existing overarching, empirical-based privacy models. Accordingly, this chapter outlines the theoretical underpinnings of the CPS model and details its core components and processes.

To demonstrate the model's utility, the OBA context is employed as a case study (as reflected in the thesis title). The OBA literature provides the point of entry through which the core elements are identified, while simultaneously revealing conceptual and empirical issues in privacy research. These elements and issues are integrated through the CPS model. Accordingly, later sections draw extensively on existing OBA research to illustrate the CPS model.

Furthermore, given the generalisable nature of privacy as a state, which is the central definitional basis of the CPS model, the model is also descriptively applied to other privacy contexts. These explorations suggest that the CPS model remains applicable across diverse scenarios, further supporting its broader relevance.

8.2 Contextual Privacy State (CPS) Model: A Definition-Driven Model



Note: The relationships specified in the CPS model are derived from the critical examinations of prior privacy conceptualisations, empirical evidence in the OBA literature, and existing privacy models. Solid lines indicate relationships identified in prior examinations, whereas dashed lines represent theoretically proposed relationships that are not reflected in these prior examinations.

Figure 7. *The Proposed Contextual Privacy State Model*

The Contextual Privacy State (CPS) model (see Figure 7) is so named to underscore the importance of defining privacy as a state. At its core, the CPS model is grounded in the conceptualisation of privacy as a heterophenomenological state (as defined in Chapter 3), meaning it is understood as an individual's fluctuating expected state that depends on external environments/situations. This foundational conceptualisation, which shifts privacy from being conceptualised as a right or control and instead

framing it as a describable personal state, shapes the structure and function of the entire model.

The CPS model draws extensively from existing privacy frameworks (see Table 14), while consciously avoiding the conceptual and structural limitations identified in the critical review. In particular, the model incorporates the Stimulus-Organism-Response (SOR) paradigm to guide its overall structure. According to SOR theory, individuals' internal responses (organism) are shaped by environmental stimuli and, in turn, influence behavioural outcomes (Bleier & Eisenbeiss, 2015; Mehrabian & Russell, 1974). Within the CPS model, environmental stimuli are acknowledged as the situational context in which the individual is embedded, and this aligns closely with Nissenbaum (2004, p. 136) principle of privacy as contextual integrity.

In the CPS model, the *expected privacy state* refers to the potential state of mind that an individual anticipates experiencing in relation to a perceived loss of control over personal information. Drawing upon the types of privacy states identified in the empirical study, individuals may express different privacy-relevant states, both intuitive and reasoning-based, when encountering different privacy contexts. Accordingly, “expected” refers to the range of possible privacy states that individuals anticipate from their own perspective, shaped by their interpretation of losing control over their information in the specific context. This *expected* state thus serves as a

subjective reference point against which the actually experienced privacy state can be evaluated.

As supported by prior literature and models, a wide array of antecedents influences individuals' privacy states. Key influencing factors are cultural norms (Kumaraguru et al., 2005; Martin & Murphy, 2017), demographic factors (Smit et al., 2014; Youn, 2005), and knowledge of the situation/context (Ham, 2017), for example, the important factor of privacy cynicism (Hoffmann et al., 2016).

Table 14. *A comparison of privacy-related factors between prior models and CPS model*

APCO model (Smith et al., 2011)			
Information privacy is "the ability of the individual to personally control information about one's self" (Stone, et al., 1983).			
Antecedents	*Factors in CPS*	*Consequences*	*Factors in CPS*
Privacy experiences	***Personal factors***	Behavioural intention	***Disclosure (vs. non-disclosure) behaviour***
Privacy awareness		Privacy calculus	***Trade-off (loss of privacy vs benefits)***
Personality differences			
Demographic differences	***Demographic factors***		
Culture/climate	***Cultural norms***		
CFIP model (Li, 2011)			
Individuals' information privacy refers to the ability of individuals to personally control information about themselves (Smith et al., 1996) (p. 454).			
Antecedents	*Factors in CPS*	*Consequences*	*Factors in CPS*

Individual factors	***Personal factors/knowledge/demographic factors***	Behavioural intention	***Disclosure (vs non-disclosure) behaviour***
Social-relational factors	***Cultural norms***	Actual behaviour	
Macro-environmental factors		Perceived privacy risks	***Trade-off (loss of privacy vs benefits)***
Organisational and task environmental factors	***Contextual situation***	Perceived benefits	
Information contingency			

SMP model (Trepte, 2021)

"I define privacy by an individual's assessments of (a) the level of access to this person in an interaction or relationship with others (people, companies, institutions) and (b) the availability of the mechanisms of control, interpersonal communication, trust, and norms for shaping this level of access through (c) self-disclosure as (almost intuitive) behavioral privacy regulation and (d)control, interpersonal communication, and deliberation as means for ensuring (a somewhat more elaborated) regulation of privacy. In social media, then, the availability of the mechanisms that can be applied to ensure privacy are crucially influenced by the content that is being shared and the social media affordances that determine how this content is further used (p. 561)".

Antecedents	*Factors in CPS*	*Consequences*	*Factors in CPS*
Individual initial assessment	***Personal factors/knowledge***	Subjective experience of privacy	***Expected privacy state***
Available privacy mechanisms			
Social media boundary conditions	***Contextual situation***	Privacy regulation behaviours	***Disclosure (vs non-disclosure) behaviour***

PPM (Dienlin, 2014)

The Privacy Process Model uses an integrated definition of privacy which is conceptualised on the core elements of three essential works on privacy (Altman, 1975; Burgoon, 1982; Westin, 1968). "Privacy emerges as the degree of separation from others (the literal definition); as a separation that can be characterised by different conditions (Westin, 1968); as being about a continuous adjustment of individual boundaries (Altman, 1975); and as taking place in four different dimensions, namely the informational, the social, the psychological and the physical (Burgoon, 1982) (p. 6)".

Antecedents	*Factors in CPS*	*Consequences*	*Factors in CPS*
Privacy context	***Contextual situation***	Self-disclosure	***Disclosure (vs non-disclosure) behaviour***
Privacy regulation (current vs the desired status)	***Expected privacy state***		

The model also explicitly incorporates the concept of *trade-offs*, a critical yet often underdeveloped element in previous frameworks. The trade-off process is derived from expectations of the expected privacy state and shaped by personal factors such as demographics (Youn, 2005), personality traits (Ozcelik & Varnali, 2019), values of privacy (Gironda & Korgaonkar, 2018), and knowledge (Ham, 2017; Van Noort et al., 2013). These factors serve as inputs into the trade-off assessment, which ultimately determines privacy-related behaviour. Importantly, the outcomes of these behaviours, whether perceived as positive or negative, feed back into personal knowledge, shaping future responses to similar privacy situations. Trade-offs are central to privacy decisions because individuals rarely disclose information without weighing perceived benefits against potential privacy loss. Models that omit or isolate trade-offs, such as Trepte's (2021) SMP, Dienlin's (2014) PPM, or even Smith et al.'s (2011) APCO, risk oversimplifying the decision-making process. To avoid the limitations of prior privacy models, the CPS model explicitly highlights the central role of trade-offs.

Notably, the CPS model also reflects and expands upon the Transparency-Awareness-Control Framework proposed by Segijn et al. (2021). Its elements are embedded within the CPS model through constructs such as knowledge of situation, personal knowledge (antecedents), as well as in the feedback loop of behaviour into personal

knowledge. This alignment illustrates how recent theoretical advancements can be integrated within the CPS framework, reinforcing its relevance and generalisability.

8.3 Contextual Privacy State (CPS) Model: OBA Case Study

Since this PhD project began with the issues of the OBA literature, using Online Behavioural Advertising (OBA) as a case study provides a valuable opportunity to demonstrate the theoretical applicability of the CPS model in a specific context. Accordingly, the following section will present OBA as a case study to illustrate how the CPS model operates in practice. In particular, existing empirical findings will be mapped onto the model to showcase the relevance and utility of its key arguments.

8.3.1 The Impact of Contexts on Privacy in the CPS Model

The CPS model acknowledges the role of contexts in shaping individuals' expected privacy state. A contextual situation refers to an external environment/situation where an individual encounters privacy concerns relevant to their privacy state. When it comes to the OBA, key contextual variables should include ad personalisation and privacy trust marks (a seal/icon on an advertisement) (Aguirre et al., 2015; Bleier & Eisenbeiss, 2015; Stanaland et al., 2011). The concept aligns with Nissenbaum's (2004) conceptual framework of privacy as contextual integrity, which emphasises defining privacy through context rather than contextual variables such as time or

location. Nissenbaum (2004) argues that in any privacy situation, if individuals perceive that their privacy has been violated based on both appropriateness and distribution, they could claim that their privacy has been violated. In this way, the CPS model helps address the previously identified issue of misspecification of contextual variables by distinguishing external contextual factors from individual social factors as a platform for defining privacy.

Nevertheless, in the CPS model, individual social factors are seen as antecedents of privacy states, not as platforms for defining privacy. The model categorises three main antecedent groups for individuals' expected privacy states: *cultural norms*, *demographics*, and *situational knowledge*. In the OBA context, cultural norms involve consumers' nationality, as European citizens have higher levels of privacy concerns than Americans (Smit et al., 2014). Demographics include factors such as gender, income, and education level (Smit et al., 2014). Knowledge factors refer to consumer perceptions of control over privacy (Gironda & Korgaonkar, 2018; Mpinganjira & Maduku, 2019), general knowledge about OBA (Smit et al., 2014), third-party data sharing (Van Eijk et al., 2012), cookies (McDonald & Cranor, 2010; Van Noort et al., 2013), ad disclosure (Leon et al., 2015; Marreiros et al., 2015; Van Noort et al., 2013), and informed privacy protection contents (Leon et al., 2012; Marreiros et al., 2015).

This classification emphasises the moderating and mediating effects between different group elements. This is an important point, as previously discussed, there will inevitably be moderating and mediating factors between different elements of the inputs in the model. For example, previous studies found that OBA knowledge directly and positively predicts American consumers' privacy concerns (Ham, 2017; Wohn et al., 2015), but barely impacts European consumers' privacy concerns (Brinson & Eastin, 2016; Smit et al., 2014; Strycharz et al., 2019). This suggests that cultural factors act as a moderator for knowledge factors. Thus, the impact of contexts in the CPS model incorporates this moderation.

8.3.2 The Central Role of the Trade-Offs in the CPS Model

The CPS model highlights that trade-offs play a central role in shaping people's privacy behaviours. The model emphasises this role in interpreting the relationships among privacy as a state, trade-offs, and privacy behaviours. There are three key aspects to this central role. First, in a privacy context, a trade-off refers to a cognitive appraisal of the benefits exchanged for a loss of privacy, which then predicts consumer privacy behaviours. Second, privacy as a state influences the outcomes of these trade-offs. Third, people's trade-offs are shaped by personal factors and knowledge. The central role of trade-offs is also suggested in Gironda and Korgaonkar's (2018) research, which found that the relationship between consumer privacy concerns and behavioural intentions (such as clicking and purchasing) is

significantly mediated by perceived invasiveness in OBA (Gironda & Korgaonkar, 2018).

The first aspect of the central role that trade-offs play is that an individual's trade-off between perceived benefits and privacy loss must occur before any privacy-related behaviour. This concept aligns with the privacy calculus theory, which posits that individuals evaluate privacy risks and benefits before engaging in any privacy-related behaviour (Laufer & Wolfe, 1977). This is of particular importance. As could be seen from the previous discussions, it would cause fragmented and inconsistent findings if there is an absence of trade-offs before any privacy behaviour.

Consistent findings in numerous OBA studies, nevertheless, support the notion that consumers weigh the trade-offs between perceived benefits and privacy loss prior to engaging in privacy-related behaviour. For example, when consumers perceive more benefits like time savings, ad relevance, usefulness, informativeness, and entertainment, they are more inclined to click on OBA ads (De Keyzer et al., 2015; Gironda & Korgaonkar, 2018; Kim & Huh, 2017; Ozcelik & Varnali, 2019; Zhu & Chang, 2016), show higher purchase intentions (Gironda & Korgaonkar, 2018), and are more willing to share personal information (Bol et al., 2018). On the other hand, if consumers feel they have lost control over their information, they tend to avoid OBA by refusing to provide personal details, leaving the OBA page, blocking OBA ads, or

opting out of OBA entirely (Baek & Morimoto, 2012; Bol et al., 2018; Ham, 2017; Jung, 2017; Nyheim et al., 2015; Strycharz et al., 2019).

Building on Laufer and Wolfe's (1977) privacy calculus theory, which suggests that privacy behaviour often correlates with self-disclosure, the CPS model categorises privacy behaviours into two types: disclosure behaviours and non-disclosure behaviours. This distinction is supported by the consolidated dimensions of privacy measurement discussed in Chapter 4, where disclosure and non-disclosure behaviours emerge as the two fundamental behavioural responses in the privacy context. In case of OBA, disclosure behaviours involve engaging with ads (e.g., clicking on ads) to share more online activity, while non-disclosure behaviours involve actions aimed at reducing exposure to ads (e.g., avoiding ads) to limit the disclosure of online activities (Baek & Morimoto, 2012; Speck & Elliott, 1997). This categorisation not only embeds theoretical validity but also addresses the fragmentation of privacy behaviour identified in Chapter 5.

The second argument regarding the central role of trade-offs is that privacy, as a state and acting as a predictor, influences these trade-offs. Treiblmaier and Pollach (2007) found that online users' expected privacy state determines their privacy trade-offs, where costs and benefits are included in the calculation of online financial communication. While this impact of privacy as a state on trade-offs has not yet been

empirically demonstrated in OBA, it could aid in understanding why perceived benefits and benefits should not be misapplied as predictors of privacy concerns (Ham, 2017; Jung, 2017; Palos-Sanchez et al., 2019; Wohn et al., 2015), and privacy concerns should not be assessed as a single aspect of perceived risks, being component of trade-offs (Bol et al., 2018; Brinson & Eastin, 2016; Zhu & Chang, 2016). As such, CPS model proposes the notion that privacy concerns influence behaviour in OBA by indicating that these effects should be illustrated through a trade-off process rather than through direct demonstration.

The third argument regarding the central role of trade-offs is that *personal factors* and *knowledge* are two antecedent groups of individuals' trade-offs. In the context of OBA, personal factors should include privacy values (Gironda & Korgaonkar, 2018), trust (Bleier & Eisenbeiss, 2015; Bol et al., 2018), and personality-derived factors, including their regulatory focus (promotion vs. prevention) (Ozcelik & Varnali, 2019). The CPS model incorporates the knowledge of OBA into the *knowledge* construct, given that previous OBA studies presented these variables as indicators of consumers' cognitive appraisal process (Ham, 2017; Strycharz et al., 2019; Van Noort et al., 2013). Most importantly, the CPS model incorporates self-efficacy into *personal knowledge* to address its misspecified effects on privacy concerns, positioning it as an antecedent of trade-offs rather than a direct antecedent of privacy concerns (Ham, 2017; Wohn et al., 2015).

Finally, in the feedback loop in the model, I consider that users' prior negative experiences with online personal information disclosure can positively shape their *personal factors* and *knowledge*, such as negative values and attitudes toward how advertisers collect and use their personal information, as well as their understanding of how online advertising works. Yang's (2013) finding reflects this loop. Although this is not a part of the central role of trade-off, it highlights a way to understand privacy behaviours and the personal factors involved with privacy.

In conclusion, the operative mechanism of the CPS model in OBA could be illustrated straightforwardly through the following scenario. Assuming the person is a young American who has become aware of OBA technologies, they will be aware that they are being tracked. If they continue browsing, they will expect a change in their privacy state to become less private. Having browsed online before without any perceived negative consequences, they will weigh that experience in their trade-off. Personal factors, such as their level of internet browsing experience, may also influence the trade-off.

8.4 CPS Model as A Generalised Privacy Model

The CPS model acknowledges that a contextual situation always exists as an external factor that shapes an individual's expected privacy state. Given this argument, the CPS model could function as a general model in any privacy-involved context, as the driven privacy definition of the model, privacy as a state, embeds contextual integrity. This means that the utility of the CPS model can be illustrated not only in OBA but also in other contexts. The following discussion focuses on explaining how the CPS model operates individual privacy in two representative contexts: physical changing rooms, and interpersonal marital couples.

To illustrate, consider the privacy context of a changing room (an open space, not booths) at a swimming pool. By entering the changing room, a person steps into a context where changing clothes may expose their naked body, potentially making private information public. Different countries have different cultural norms about being naked in public spaces (Smith, 1980), which can influence how individuals perceive the situation and the extent to which they feel a loss of privacy. As most people are familiar with changing rooms, the expectation will be that there is a potential for some loss of privacy and, thus, a potential change in the state of privacy (e.g., another person enters the changing room). If the person has previously used a changing room without experiencing negative effects from the loss of privacy, they may weigh that experience in a trade-off, choosing to lose some privacy in exchange

for the ability to swim. Assuming there are no negative consequences during this occasion, future trade-offs in similar situations will likely be easier to make.

The model also generalised privacy issues in the context of marital relationships, which is the basis of Petronio's (1991) Communication Privacy Management (CPM) theory. By sharing private information with their partner, a person moves into a context where the partner keeps their information private or discloses it to the public. As a result, the individual's privacy state may change depending on how their partner handles the private information. If the partner shares the information with friends, especially those with whom the individual is not close, the expectation of privacy loss would be significant. However, before they conduct further disclosure or non-disclosure behaviour with their partner, they will balance the risk of giving up privacy (e.g. break up with their partners) and the perceived benefits (e.g. maintaining this relationship), whereby their personalities would come into effect. Assuming the need to maintain the relationship, they may choose to withhold private information in future similar situations to protect their privacy.

8.5 Conclusion

The Contextual Privacy State (CPS) model offers a conceptually robust and cognitively successful framework for understanding consumer privacy within Online Behavioural Advertising (OBA). Grounded in the conceptualisation of privacy as a heterophenomenological state, the CPS model captures the context-generalisable nature of privacy. It also incorporates valuable elements from empirical research, theoretical models, and privacy definitions, while avoiding key limitations found in earlier critical examinations of empirical findings and models. These philosophical underpinnings support the cognitive reliability of the CPS model.

Its application to the OBA context demonstrates the model's explanatory power in accounting for consumer privacy in OBA, demonstrating its superior theoretical outcomes in a specific context. Moreover, its extension to offline and interpersonal privacy scenarios further highlights its context-generalisable nature. As such, the CPS model functions as a broadly applicable structure for analysing privacy behaviour across OBA and beyond. The advancement of the CPS benefits from the integration of prior empirical and theoretical advantages while mitigating earlier shortcomings. Through these analyses, the CPS model emerges as a generative framework for rethinking privacy in ways that are cognitively congruent with the complexities of everyday life.

Chapter 9: Discussions and Conclusions

9.1 Introduction

Building on prior work, this primarily conceptual thesis contributes to a clearer understanding of consumer privacy within the context of online behavioural advertising (OBA). A closer examination of privacy research in OBA, both in terms of its conceptual foundations and the empirical evidence supporting it, reveals some fundamental questions about its cognitive success (Niiniluoto, 1999). Central to this inquiry is questioning the dominant conceptualisation of privacy as control, which is a framework widely applied in OBA. It raises the question: if this framework does not adequately reflect the complexities of privacy, how can the alternative existing conceptual approaches stemming from Smith et al. (2011) provide a more accurate representation? As such, in the following section, I will discuss how both the conceptualisation of privacy and empirical evidence in OBA are theoretically incoherent and demonstrate how this PhD project has resolved them by advancing a re-conceptualisation of privacy as a state.

9.2 Discussions

Chapter 4 critically examines four main strands of privacy conceptualisation categorised by Smith et al. (2011). The examination suggests that the dominant conceptualisation of privacy as control, which has been observed in Chapter 2, sits on

shaky definitional foundations and suffers from insufficient measurement. These issues also extend to the conceptualisations of privacy as a right and as a commodity. Among these, one conceptualisation stands out as more compelling in capturing the reality of individual privacy: privacy as a state, which Dennett (2007, p. 249) describes as "a level of first-person description of the conscious dimension of cognitive properties, corresponding to the phenomenological properties of cognition". Interestingly, this state-based conceptualisation surfaces in some OBA studies, such as Aguirre et al. (2015) and Phelan et al. (2016), yet it remains remarkably underrepresented in empirical findings.

One possible explanation for this neglect lies in the entrenched dominance of the "privacy as control" conceptualisation approach in OBA research. OBA research involves the premature application of existing privacy measurements without sufficient thematic groundwork, often fails to account for the substantial erosion of individuals' practical control due to pervasive tracking technologies employed in OBA (Büchi et al., 2022; Strycharz & Segijn, 2022) and to recognise that the measurements do not assess control *per se*, but instead reflect privacy states, values, attitudes, and behavioural intentions. As Avis and Henderson (2022) caution, when the measurements fail to reflect what is defined accurately, they hinder sound theory development in the corresponding field.

In light of these limitations, Chapter 4 advocates a conceptual shift from defining privacy as control to a state. This approach better captures heterophenomenological (Dennett, 2007) and psychological (Stuart et al., 2019) dimensions of privacy, aligning with how individuals actually experience privacy (Margulis, 2003). Crucially, echoing Koops et al. (2016) and Laufer and Wolfe (1977), defining privacy as a state allows for a cleaner separation between privacy itself as a state and its antecedents, such as values, attitudes, and perceived control, thereby reducing conceptual confusion in measurement. This thesis, therefore, argues that the state-based conceptualisation offers potential for greater cognitive success in capturing individual privacy experience.

This argument is further supported by the empirical findings from Chapter 7. These results show that individuals experience privacy invasions through a spectrum of intuitive and reasoning psychological states across online, offline, and interpersonal contexts. Intuitive feelings, such as feeling *creepy* or *monitored*, emerge as automatic, emotionally charged responses to perceived privacy violations. In contrast, reasoning feelings, such as feeling *risky* or *insecure*, are based on more reflective, cognitive evaluations of potential risks associated with privacy invasions. This distinction illustrates that privacy involves multifaced and layered psychological experiences, not simply a rational assessment of control over information.

Building on this foundational critique, the research expands the focus to empirical studies on consumer privacy concerns in OBA, as analysed in Chapters 3 and 5. This shift moves from questioning *what* privacy is to examining *how* privacy is studied and evidenced in practice. As the thesis reveals, conceptual issues also manifest in empirical fragmentation and inconsistencies. Specifically, many empirical studies conflate external and individual factors under the term "context" when defining privacy, misuse cognitive appraisals as direct predictors of privacy concerns, and overlook privacy trade-offs as the core of shaping behaviour. These missteps contribute to conflicting findings that fail to accurately capture privacy experience.

The cognitive issues identified in the conceptualisation of privacy and the interpretation of empirical findings in OBA underscore a critical point: a cognitively successful understanding of privacy is essential. Simply put, if existing definitions and empirical evidence fail to reflect the realism of privacy in OBA, then the foundational positions of widely used privacy models, which aim to guide further empirical research, must be questioned. This argument is detailed in Chapter 6, which demonstrates that prevailing models suffer from the same conceptual and evidentiary shortcomings as the literature in OBA.

In the absence of a model that successfully explains how privacy operates in the real world of OBA, the legitimacy of existing privacy frameworks as overarching theories

becomes increasingly questionable. In response, Chapter 8 introduces the Contextual Privacy State (CPS) model as a theoretically and cognitively coherent alternative. Developed through rigorous analysis of defining privacy as a state, an examination of existing privacy models, and a synthesis of empirical findings, the CPS model offers a scientifically grounded rethinking of how privacy should be conceptualised and studied in OBA.

Most significantly, responding to Nissenbaum's (2004) theory of contextual integrity, this thesis moves beyond the confines of OBA to propose a generalisable conceptualisation of privacy that applies across diverse contexts. Although this broader applicability is not the primary focus of the thesis, it offers a valuable perspective for addressing a long-standing and fundamental debate in privacy research: the nature of privacy itself. As the field continues to mature, scholars remain divided over whether privacy should be examined within specific contexts or understood through the broader lens (Smith et al., 2011). In other words, does privacy inherently possess a context-specific nature, or is it generalisable across different settings? This thesis contends that such a dichotomy can be reconciled by redefining privacy as a state

As shown in Chapter 4, defining privacy as a state provides a robust response to critiques: "General privacy is so dependent on the specific context that it is impossible

to develop a one-size-fits-all conceptualisation of general privacy (Smith et al., 2011, p. 1002)“. However, the state-based perspective reframes this problem: while the type and intensity of psychological privacy states may vary across contexts, the underlying phenomenon, that is, privacy as a heterophenomenological experience, remains constant. In other words, it is not the existence of privacy as a state that changes, but how it is experienced and expressed in different settings.

Chapter 7 illustrates this with empirical evidence showing that certain privacy states are applicable across diverse contexts, including OBA, changing rooms, and interpersonal relationships, albeit with differing frequencies and intensities. This demonstrates patterns of continuity and variation in privacy states across contexts. Furthermore, the justification in Chapter 8 of how the Contextual Privacy State (CPS) model applies across the above contexts also reinforces the notion that privacy is contextually generalisable. Taken together, these results suggest that while the intensity of privacy states may differ between online, offline, and interpersonal settings, the underlying concept of a privacy state remains broadly applicable across contexts.

9.3 Contributions

The thesis is the first work to provide such a comprehensive critique of the existing conceptual foundations of and empirical evidence for consumer privacy in OBA. Using the results of the critical analysis, it proposes a cognitively successful conceptualisation approach to privacy. Building directly on the critical arguments and empirical findings outlined in the previous section, this thesis makes several significant contributions to the conceptualisation, empirical understanding, and theoretical modelling of consumer privacy, particularly within the context of Online Behavioural Advertising (OBA), but also extending beyond it.

The first key contribution lies in the reconceptualisation of privacy. Chapter 2 and 4 challenge the widely accepted conceptualisation of privacy as control, revealing its theoretical fragility and limited empirical relevance. This control-based model has been criticised for ignoring the realities of contemporary digital environments, where pervasive data collection and surveillance leave online users with little to no control over their privacy and information. Rooted in an economic rationale, it also neglects the social value of privacy. In contrast, reconceptualising privacy as a state addresses these shortcomings by framing it as a heterophenomenological mental state: one that individuals can meaningfully describe based on their subjective experience within a given context. By foregrounding the practical and social value of privacy, this state-based approach not only clears the murkiness of privacy's conceptual and theoretical

foundation but also offers a more cognitively coherent framework for re-examining privacy.

This conceptual shift is empirically validated in Chapter 7, which employs a mixed-methods approach to identify specific privacy states that individuals experience in response to OBA. These include intuitive states (e.g., *creepy*, *monitored*, or *annoyed*) and reasoning-based states (e.g., *risky*, *insecure* or *manipulated*). These findings mark a substantial theoretical advancement by demonstrating that privacy is a layered self-described state experience, encompassing both automatic emotional and cognitive responses. The identification of these measurable states reinforces the validity of conceptualising privacy as a heterophenomenological state. This dual perspective of state types offers a novel lens for OBA research to more accurately interpret and measure consumer privacy responses.

Moreover, the quantitative phase of the mixed-methods study confirms that these privacy states, particularly intuitive feelings like feeling *creepy*, *annoyed*, and *monitored*, and reasoning feelings like being *risky*, *manipulated*, and *insecure*, are not confined to OBA but generalisable across diverse privacy-involved environments. This empirically supports the generalisable nature of privacy as a state. As such, this chapter contributes to the exploratory sequential design through additional empirical

application of the method, while empirically substantiating the generalisability and two-dimensional structure of privacy as a state.

Further contributions arise from the empirical critique of OBA privacy research presented in Chapters 3 and 5. Chapter 3 offers the first systematic synthesis of empirical studies on consumer privacy concerns specific to OBA, highlighting the fragmentations of the antecedents and outcomes while revealing notable inconsistencies in findings related to demographics, ad characteristics, consumer knowledge, and behaviours. This fills a critical gap in the literature, as no prior literature review has focused exclusively on consumer privacy concerns within the OBA context. By identifying the fragmentation and inconsistencies, the chapter highlights the pressing need for a more unified and theoretically robust approach to studying privacy in this domain.

Chapter 5 criticises the inconsistencies by pinpointing four significant sources of theoretical confusion. It disentangles external contextual factors from individual-level social factors, which are often conflated under the label of "context" in existing empirical research. In addition, it reexamines the role of cognitive appraisal variables and the trade-offs, which have been mis specified and overlooked in predicting privacy behaviour. Together, these insights help explain the field's fragmented

findings and offer more precise conceptual and theoretical foundations to guide future empirical research.

The thesis's final and perhaps most integrative contribution is the development of the Contextual Privacy State (CPS) model, introduced in Chapter 8. Grounded in the conceptualisation of privacy as a heterophenomenological state, the CPS model provides a coherent and cognitively informed framework for analysing how individuals perceive and respond to privacy violations within OBA and across broader contexts. The CPS model makes two major contributions. First, it directly addresses the core theoretical limitations identified in Chapters 4, 5 and 6, including the lack of conceptual clarity, the conflated impact of context, and the neglect of trade-offs as central to privacy decision-making. Specifically, it clarifies the roles of confounding contextual variables by categorising them into contextual situations and antecedents of individual privacy, thereby disentangling their distinct influences on privacy states. The model also acknowledges the central role of trade-offs in shaping consumer reactions to OBA. It emphasises that before engaging in any privacy-related behaviour, consumers assess a trade-off between potential privacy loss and perceived benefits, including personalised ads, relevant content or improved alignment with their interests. The extent to which consumers feel their privacy has been violated shapes this trade-off. By integrating these elements, the CPS model advances a more consistent and nuanced understanding of consumer privacy in OBA.

Second, the CPS model holds broader theoretical significance beyond OBA. It provides a coherent framework for analysing individual privacy across diverse domains, including online targeted advertising, social relationships, and public space surveillance. By conceptualising privacy as a dynamic and generalisable state, the model explains why privacy responses vary across contexts without sacrificing conceptual coherence. For example, whether individuals are deciding to share health data with an app, enable location tracking, or accept targeted advertising, their decisions are driven by comparable internal trade-offs shaped by their momentary privacy state. Thus, the CPS model offers a context-generalisable, theoretically robust approach to understanding individual privacy behaviours across a wide range of settings.

The thesis also provides managerial implications for the OBA industry in terms of advertisers, privacy practitioners, and regulators. Firstly, before designing privacy regulations, regulators should clearly understand the types of privacy states that consumers may experience and the role of the various factors that influence individuals in determining these states. For example, the empirical findings of this thesis show that when encountering OBA, consumers are significantly more likely to experience privacy states such as feeling *uneasy*, and *manupulated* compared with every day and interpersonal contexts. Therefore, when developing privacy

regulations, regulators should place greater emphasis on protecting consumers from experiencing such negative privacy states by considering any contextual factors that may trigger them.

In this thesis, the importance of trade-offs in shaping privacy disclosure behaviour is strongly highlighted. Accordingly, regulators should focus on ensuring that consumers are making informed trade-offs. The CPS model provides an easily comprehended overview of the factors that work towards the trade-offs, for example, the notion that individuals enter into a privacy context with expectations over the alteration of their privacy state, and that those expectations are, in part, derived from experience. It is also pivotal for companies to understand consumer privacy state boundaries and how those boundaries will impact consumer behaviour under different contexts. By making the trade-off explicit and using a process of informed consent, companies may, in the long run, be able to gain greater levels of trust from consumers.

It should be noted that privacy states are closely related to a general lack of trust and irritation with online advertising, which has, for example, seen the widespread adoption of ad-blocking software. This is a significant problem for advertisers (Santoso et al., 2020). For the companies serving advertisements, I advise them to grasp the need for ad personalisation and ad disclosure. In doing so, advertisers may also gain greater levels of trust from consumers. Although ad blocking is partly driven

by ad intrusiveness (Santoso et al. 2020), improving trust would also help ameliorate problems such as ad blocking.

Collectively, these contributions represent a foundational step toward rethinking consumer privacy, both within the context of OBA and even more broadly. By offering re-examined conceptual framework, empirical validation, comprehensive theoretical critique, and a theoretically grounded model, this thesis not only addresses notable theoretical gaps but also brings to light emerging yet previously overlooked issues in the OBA literature and industry. In doing so, the research provides not only theoretical contributions but also broader practical relevance by offering a clearer framework through which regulators, advertisers, and privacy practitioners may better understand how consumers experience privacy in OBA contexts and how privacy-related trade-offs shape consumer behaviour.

The reconceptualisation of privacy as a state opens up new opportunities for further theoretical development, methodological application, and empirical exploration across a range of contexts. Building on these efforts, the following section outlines several avenues for future research that can extend, refine, and apply the insights generated in this study.

9.4 Future Research

Aligning with the conceptual nature of this PhD thesis, the most compelling future direction for the research lies in two critical reviews: one focuses on the conceptualisation of privacy, and the other on the empirical findings that build upon it. These reviews aim to critically examine the theoretical foundations and evolution of consumer privacy in the context of OBA, identifying how and why the dominant conceptualisations of privacy are theoretically problematic and the causes that contribute to fragmented and inconsistent empirical evidence. The first task is largely conceptual, which is to critically analyse how key concepts and empirical findings have been used, and how their use has contributed to shaping a complex and problematic entity (Avis & Henderson, 2022). This conceptual groundwork could be further applied to examining other privacy-related issues, such as privacy paradox (Strycharz & Segijn, 2022), privacy cynicism (Hoffmann et al., 2016), and surveillance-related beliefs (Büchi et al., 2022).

The critical examination of Smith et al.'s (2011) main streams of privacy conceptualisations should be purposeful. As was identified in the Chapter 4, three of the four privacy conceptualisations, including privacy as a right, privacy as commodity, and privacy as control, are problematic in coherently reflect the reality of consumer privacy. Instead, privacy as a state offers greater cognitive success in capturing individual heterophenomenological cognition of privacy experience

(Dennett, 2007) while incorporating privacy's social value (Hull, 2015). As such, the thesis suggests a transition to conceptualise privacy as a state. This outcome of the critical examinations of privacy conceptualisations provides opportunities to create a firmer foundation for the development of privacy knowledge and theory. Considering the contextual generalisable nature of privacy as a state, further research should critically examine whether conceptualising privacy as a state suit in alternative digital environments, such as social media platforms or smart device ecosystems, thereby broadening the theoretical understanding of privacy beyond OBA.

An additional imperative lies in the development of robust measures of privacy as a state. The mixed-methods research demonstrates that both intuitive and reasoning descriptors are fundamental to understanding how individual heterophenomenological experience privacy. Accordingly, future research should prioritise the development and validation of psychometrically sound scales that can capture these dual dimensions of privacy states. Additionally, the mixed-methods research demonstrates that participants from multiple cultural contexts, the US, China, and New Zealand, show different states and levels of privacy state, future studies could benefit from a deeper exploration of cultural differences in privacy states. For instance, different cultural norms regarding privacy may influence the intensity and type of privacy states experienced in various contexts. If this is to serve as a foundational concept in privacy research, rigorous cross-contextual testing and examination will be required.

The study's quantitative findings in Chapter 7 reveal a notable difference in the number of generalisable intuitive descriptors and reasoning descriptors. Specifically, a greater number of intuitive descriptors were found to be significantly associated with contexts, while only three reasoning descriptors demonstrated significant associations. Therefore, future research can leverage this distinction to explore why individuals express more intuitive feelings in private settings and examine the specific connection between these intuitive feelings and reasoning-based feelings.

The third avenue for research is to investigate the CPS model. The development of the CPS model will provide a solid foundation for research. As was argued in Chapter 8, the CPS model is positioned as a generalisable framework applicable to diverse privacy contexts. However, the model has not yet been used as a foundational framework for privacy research and still requires empirical validation. For the model to serve as a key foundation for privacy research, it needs to undergo rigorous testing and examination. Therefore, future work should aim to systematically test the CPS model across multiple domains, including digital platforms (e.g., social media, OBA), physical environments (e.g., public surveillance), and interpersonal interactions. Additionally, as proposed cultural norms influence the intensity and type of privacy states, cross-cultural application of the model will be critical to determining its adaptability and relevance would be beneficial.

The CPS model highlights the importance of contextual situations influences on privacy states. Future research would be beneficial to explore how external situational factors, such as informed consent protocols, privacy policy, ad disclosure icons, and ad blockers (Brinson & Eastin, 2016), affect privacy trade-offs and subsequent behaviours.

Another promising area for exploration involves the central role of trade-offs to the CPS model. A key element of the CPS is that consumers are making trade-offs, and there is a broad scope for examining how expected privacy states play into these trade-off. For instance, examining the role of intuitive versus reasoning-based privacy states in this process will provide deeper insights into the psychological mechanisms that drive privacy behaviours. In the CPS model, the trade-off is an important mediator of the consumer's expected privacy state and behaviour. Future studies should focus on its antecedents, thereby providing a comprehensive understanding of this mediator. The model shows that a consumer's trade-off is rooted in personal factors and shaped by their expected privacy state. Therefore, future research could investigate the relationship between the consumer's expected privacy state and their trade-off decisions or examine how different personal factors influence the trade-off process. For example, further studies could examine how consumers' attitudes and values towards privacy shape the trade-off process in the context of OBA.

Overall, the directions and examples given above are just starting points. Also, as the work in this PhD thesis enters the body of privacy literature in OBA, it may be that other researchers and theorists might also find new avenues to explore as a result of critical reviews of the conceptualisation of privacy, empirical research, and prior privacy models presented in the chapters.

9.5 Conclusion

In this PhD project, the theoretical flaws in consumer privacy research within OBA, particularly from conceptual and empirical viewpoints, have been critically and rigorously observed. Transiting to conceptualise privacy as a state and the development of the Contextual Privacy State model have been presented to resolve these issues. Although OBA raised these issues, the nature of these two main solutions can lead to a more unified scholarly understanding of border privacy fields.

By critically engaging with the theoretical cognitive success of privacy conceptualisation and scrutinising the empirical findings built upon them, this PhD thesis marks the first bold departure from the dominant orthodoxy that frames marketing, particularly advertising, as a purely practical discipline. In doing so, it challenges the disciplinary boundaries that have long limited theoretical innovation.

Reference

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

Afifi, T. D. (2003). 'Feeling caught'in stepfamilies: Managing boundary turbulence through appropriate communication privacy rules. *Journal of Social and Personal Relationships*, *20*(6), 729–755.

Aguinis, H., & Bradley, K. J. (2014). Best practice recommendations for designing and implementing experimental vignette methodology studies. *Organizational Research Methods*, *17*(4), 351–371.

Aguirre, E., Mahr, D., Grewal, D., De Ruyter, K., & Wetzels, M. (2015). Unraveling the personalization paradox: The effect of information collection and trust–building strategies on online advertisement effectiveness. *Journal of Retailing*, *91*(1), 34–49.

Altman, J., Nissim, K., & McDonald, A. M. (2011). *Regulating online behavioral advertising: Programs, policies, and technologies*. Carnegie Mellon University.

An, S., Kim, H., & Park, J. (2018). Advertising companies' privacy policies and consumers' perceived transparency in online behavioral advertising. *Journal of Advertising, 47*(4), 345–358.

Avis, M., & Henderson, I. L. (2022). A solution to the problem of brand definition. *European Journal of Marketing*, *56*(2), 351–374.

Avis, M., Aitken, R., & Ferguson, S. (2012). Brand relationship and personality theory: Metaphor or consumer perceptual reality? *Marketing Theory, 12*(3), 311–331.

Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly*, *30*(1), 13–28.

Baek, T. H., & Morimoto, M. (2012). Stay away from me. *Journal of Advertising*, *41*(1), 59–76.

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

Basinger, E. D., Wehrman, E. C., & McAninch, K. G. (2016). Grief communication and privacy rules: Examining the communication of individuals bereaved by the death of a family member. *Journal of Family Communication*, *16*(4), 285–302.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, *35*(4), 1017–1041.

Bevan, M. T. (2014). A method of phenomenological interviewing. *Qualitative Health Research*, *24*(1), 136–144.

Bleier, A., & Eisenbeiss, M. (2015). The importance of trust for personalized online advertising. *Journal of Retailing*, *91*(3), 390–409.

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2017). Online behavioral advertising: A literature review and research agenda. *Journal of Advertising*, *46*(3), 363–376.

Bol, N., Dienlin, T., Kruikemeier, S., Sax, M., Boerman, S. C., Strycharz, J., Helberger, N., & De Vreese, C. H. (2018). Understanding the effects of personalization as a privacy calculus: Analyzing self–disclosure across health, news, and commerce contexts. *Journal of Computer–Mediated Communication*, *23*(6), 370–388.

Borgesius, F. Z. (2013). *Behavioral targeting: A European legal perspective*. Springer.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101.

Brinson, N. H., & Eastin, M. S. (2016). Juxtaposing the persuasion knowledge model and privacy paradox: An experimental look at advertising personalization, public policy and public understanding. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *10*(1), Article 1.

Brinson, N. H., Eastin, M. S., & Bright, L. F. (2019). Advertising in a quantified world: A proposed model of consumer trust, attitude toward personalized advertising and outcome expectancies. *Journal of Current Issues & Research in Advertising*, *40*(1), 54–72.

Brown, S. (2002). Vote, vote, vote for Philip Kotler. *European Journal of Marketing*, *36*(3), 313–324.

Büchi, M., Festic, N., & Latzer, M. (2022). The chilling effects of digital

dataveillance: A theoretical model and an empirical research agenda. *Big Data & Society*, *9*(1), 20539517211065368.

Burgoon, J. K., Parrott, R., Le Poire, B. A., Kelley, D. L., Walther, J. B., & Perry, D. (1989). Maintaining and restoring privacy through communication in different types of relationships. *Journal of Social and Personal Relationships*, *6*(2), 131–158.

Busetto, L., Wick, W., & Gumbinger, C. (2020). How to use and assess qualitative research methods. *Neurological Research and Practice*, *2*(1), Article 14.

Cornelissen, J. P. (2003). Metaphor as a method in the domain of marketing. *Psychology & Marketing*, *20*(3), 209–225.

Creswell, J. W., & Plano Clark, V. L. (2017). *Designing and conducting mixed methods research* (3rd ed.). SAGE Publications.

De Keyzer, F., Dens, N., & De Pelsmacker, P. (2015). Is this for me? How consumers respond to personalized advertising on social network sites. *Journal of Interactive Advertising*, *15*(2), 124–134.

Dennett, D. C. (1993). Consciousness explained. *Journal of Philosophy, 90*(4), 190–229.

Dennett, D. C. (2007). Heterophenomenology reconsidered. *Phenomenology and the Cognitive Sciences*, *6*(3), 247–270.

Dienlin, T. (2014). The privacy process model. In H. Quandt & S. Kröger (Eds.), *Medien und Privatheit* (pp. 105–122). Springer VS.

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents:

Measurement validity and a regression model. *Behaviour & Information Technology, 23*(6), 413–422.

Dolnicar, S., & Jordaan, Y. (2007). A market–oriented approach to responsibly managing information privacy concerns in direct marketing. *Journal of Advertising*, *36*(2), 123–149.

Dourish, P., & Anderson, K. (2006). Collective information practice: Exploring privacy and security as social and cultural phenomena. *Human–Computer Interaction*, *21*(3), 319–342.

Dwivedi, Y. K., et al. (2021). Setting the future of digital and social media marketing research: Perspectives and research propositions. *Journal of Business Research*, 125, 757–772.

Field, A. (2024). *Discovering statistics using IBM SPSS statistics* (6th ed.). SAGE Publications Ltd.

Foucault, M. (1982). The subject and power. In H. L. Dreyfus & P. Rabinow (Eds.), *Michel Foucault: Beyond structuralism and hermeneutics* (2nd ed., pp. 208–226). University of Chicago Press.

Foucault, M. (1985). *The use of pleasure: The history of sexuality* (Vol. 2, R. Hurley, Trans.). Pantheon Books.

Fratini, A., & Hemer, S. R. (2020). Broadcasting your death through livestreaming: Understanding cybersuicide through concepts of performance. *Culture, Medicine, and Psychiatry, 44*(4), 524–543.

Gironda, J. T., & Korgaonkar, P. K. (2018). iSpy? Tailored versus invasive ads and

consumers' perceptions of personalized advertising. *Electronic Commerce Research and Applications, 29*(C), 64–77.

Haber, P. (2012). Perceptions of leadership: An examination of college students' understandings of the concept of leadership. *Journal of Leadership Education*, *11*(2), 26–51.

Ham, C.–D. (2017). Exploring how consumers cope with online behavioral advertising. *International Journal of Advertising*, *36*(4), 632–658.

Ham, C.-D., & Nelson, M. R. (2016). The role of persuasion knowledge, assessment of benefit and harm, and third-person perception in coping with online behavioral advertising. *Computers in Human Behavior, 62*, 689–702.

Hasenbush, A., Flores, A. R., & Herman, J. L. (2019). Gender identity nondiscrimination laws in public accommodations: A review of evidence regarding safety and privacy in public restrooms, locker rooms, and changing rooms. *Sexuality Research and Social Policy*, *16*(1), 70–83.

Hoffmann, C. P., Lutz, C., & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 10*(4), Article 7.

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

Hu, H., Xu, A., Wang, Z., Gao, C., & Wu, X. (2025). Self–management behaviours in rheumatoid arthritis patients: What role do health beliefs play? *International Journal of Nursing Practice*, *31*(1), e13320.

Hull, G. (2015). Successful failure: What Foucault can teach us about privacy self-management in a world of Facebook and big data. *Ethics and Information Technology, 17*(2), 89–101.

Hunt, S. D. (2003). *Controversy in marketing theory: For reason, realism, truth, and objectivity*. M. E. Sharpe.

Jarvis, C. B., MacKenzie, S. B., & Podsakoff, P. M. (2003). A critical review of construct indicators and measurement model misspecification in marketing and consumer research. *Journal of Consumer Research, 30*(2), 199–218.

Johnson, R. B., Onwuegbuzie, A. J., & Turner, L. A. (2007). Toward a definition of mixed methods research. *Journal of Mixed Methods Research, 1*(2), 112–133.

Jung, A.-R. (2017). The influence of perceived ad relevance on social media advertising: An empirical examination of a mediating role of privacy concern. *Computers in Human Behavior, 70*, 303–309.

Kahneman, D., & Tversky, A. (2013). Prospect theory: An analysis of decision under risk. In L. C. MacLean & W. T. Ziemba (Eds.), *Handbook of the fundamentals of financial decision making: Part I* (pp. 99–127). World Scientific.

Keszey, T. (2020). Behavioural intention to use autonomous vehicles: Systematic review and empirical extension. *Transportation Research Part C: Emerging Technologies, 119*, Article 102732.

Kim, H., & Huh, J. (2017). Perceived relevance and privacy concern regarding online behavioral advertising (OBA) and their role in consumer responses. J*ournal of Current Issues & Research in Advertising, 38*(1), 92–105.

Koops, B.-J., Newell, B. C., Timan, T., Skorvanek, I., Chokrevski, T., & Galič, M. (2016). A typology of privacy. *University of Pennsylvania Journal of International Law, 38*(2), 483–575.

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

Kumaraguru, P., Cranor, L. F., & Newton, E. (2005). Privacy perceptions in India and the United States: An interview study. In *Proceedings of the 33rd Research Conference on Communication, Information and Internet Policy (TPRC)*.

Lambert, S. (2012). The perception and implementation of sustainable leadership strategies in further education colleges. *Journal of Leadership Education, 11*(2), 102–120.

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

Leon, P. G., Cranshaw, J., Cranor, L. F., Graves, J., Hastak, M., Ur, B., & Xu, G. (2012). What do online behavioral advertising privacy disclosures communicate to users? In *Proceedings of the 2012 ACM Workshop on Privacy in the Electronic Society (WPES '12)* (pp. 19–30). Association for Computing Machinery.

Leon, P. G., Rao, A., Schaub, F., Marsh, A., Cranor, L. F., & Sadeh, N. (2015). Privacy and behavioral advertising: Towards meeting users' preferences. In

Proceedings of the Eleventh Symposium on Usable Privacy and Security (SOUPS 2015) (pp. 5–20). USENIX Association.

Li, Y. (2011). Empirical studies on online information privacy concerns: Literature review and an integrative framework. *Communications of the Association for Information Systems, 28*(1), Article 28.

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

Li, Y. (2014). A multi–level model of individual information privacy beliefs. *Electronic Commerce Research and Applications, 13*(1), 32–44.

Liyanaarachchi, G. (2020). Online privacy as an integral component of strategy: allaying customer fears and building loyalty. *Journal of Business Strategy*, *41*(5), 47–56.

MacKenzie, S. B. (2003). The dangers of poor construct conceptualization. *Journal of the Academy of Marketing Science, 31*(3), 323–326.

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

Malterud, K., Siersma, V. D., & Guassora, A. D. (2016). Sample size in qualitative interview studies: Guided by information power. *Qualitative Health Research, 26*(13), 1753–1760.

Margulis, S. T. (1977). Conceptions of privacy: Current status and next steps. *Journal of Social Issues, 33*(3), 5–21.

Margulis, S. T. (2003). On the status and contribution of Westin's and Altman's theories of privacy. *Journal of Social Issues, 59*(2), 411–429.

Marreiros, H., Gomer, R., Vlassopoulos, M., & Tonin, M. (2015). Exploring user perceptions of online privacy disclosures. In *Proceedings of the Sixteenth ACM Conference on Economics and Computation (EC '15)* (pp. 823–823). Association for Computing Machinery.

Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science, 45*(2), 135–155.

Maseeh, H. I., Jebarajakirthy, C., Pentecost, R., Arli, D., Weaven, S., & Ashaduzzaman, M. (2021). Privacy concerns in e-commerce: A multilevel meta-analysis. *Psychology & Marketing*, *38*(10), 1779–1798.

Maseeh, H. I., Nahar, S., Jebarajakirthy, C., Ross, M., Arli, D., Das, M., ... & Ashraf, H. A. (2023). Exploring the privacy concerns of smartphone app users: a qualitative approach. Marketing Intelligence & Planning, 41(7), 945-969.

McDonald, A. M., & Cranor, L. F. (2010). Americans' attitudes about internet behavioral advertising practices. In *Proceedings of the 9th Annual ACM Workshop on Privacy in the Electronic Society (WPES '10)* (pp. 63–72). Association for Computing Machinery.

Meho, L. I., & Yang, K. (2007). Impact of data sources on citation counts and rankings of LIS faculty: Web of Science versus Scopus and Google Scholar. *Journal of the American Society for Information Science and Technology, 58*(13), 2105–2125.

Menard, S. (2001). *Applied logistic regression analysis* (2nd ed.). SAGE Publications.

Morse, J. M., Hupcey, J. E., & Cerdas, M. (1996). Criteria for concept evaluation. *Journal of Advanced Nursing, 24*(2), 385–390.

Mowday, R. T., & Sutton, R. I. (1993). Organizational behavior: Linking individuals and groups to organizational contexts. *Annual Review of Psychology, 44*(1), 195–229.

Mpinganjira, M., & Maduku, D. K. (2019). Ethics of mobile behavioral advertising: Antecedents and outcomes of perceived ethical value of advertised brands. *Journal of Business Research, 95*, 464–478.

Muller, D., Judd, C. M., & Yzerbyt, V. Y. (2005). When moderation is mediated and mediation is moderated. *Journal of Personality and Social Psychology, 89*(6), 852–863.

Niiniluoto, I. (1999). *Critical scientific realism*. Oxford University Press.

Nill, A., & Aalberts, R. J. (2014). Legal and ethical challenges of online behavioral targeting in advertising. *Journal of Current Issues & Research in Advertising, 35*(2), 126–146.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review, 79*(1), 119–157.

Noor, U., Awan, T., & Zahid, M. (2019). Examining the impact of personalization on online advertising engagement: Moderating role of privacy concerns of online users. *Business Review, 14*(2), 31–46.

Nyheim, P., Xu, S., Zhang, L., & Mattila, A. S. (2015). Predictors of avoidance

towards personalization of restaurant smartphone advertising: A study from the Millennials' perspective. *Journal of Hospitality and Tourism Technology, 6*(2), 145–159.

Ozcelik, A. B., & Varnali, K. (2019). Effectiveness of online behavioral targeting: A psychological perspective. *Electronic Commerce Research and Applications, 33*, Article 100819.

Palos–Sanchez, P., Saura, J. R., & Martin–Velicia, F. (2019). A study of the effects of programmatic advertising on users' concerns about privacy overtime. *Journal of Business Research, 96,* 61–72.

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

Petronio, S., & Child, J. T. (2020). Conceptualization and operationalization: Utility of communication privacy management theory. *Current Opinion in Psychology, 31*, 76–82.

Phelan, C., Lampe, C., & Resnick, P. (2016). It's creepy, but it doesn't bother me. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (pp. 5240–5251). Association for Computing Machinery.

Rodgers, S., & Thorson, E. (2000). The interactive advertising model: How users perceive and process online ads. *Journal of Interactive Advertising, 1*(1), 41–60.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude

change. *The Journal of Psychology*, *91*(1), 93–114.

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. T. Cacioppo & R. E. Petty (Eds.), *Social psychophysiology: A sourcebook* (pp. 153–176). Guilford Press.

Santoso, I., Wright, M., Trinh, G., & Avis, M. (2020). Is digital advertising effective under conditions of low attention?. *Journal of Marketing Management*, *36*(17–18), 1707–1730.

Schaub, F., Marella, A., Kalvani, P., Ur, B., Pan, C., Forney, E., & Cranor, L. F. (2016). Watching them watching me: Browser extensions' impact on user privacy awareness and concern. In *Proceedings of the 2016 NDSS Workshop on Usable Security (USEC)*. Internet Society.

Schoeman, F. D. (Ed.). (1984). *Philosophical dimensions of privacy: An anthology*. Cambridge University Press.

Scott, E. M. (2013). Protecting consumer data while allowing the web to develop self-sustaining architecture: Is a trans-Atlantic browser-based opt-in for behavioral tracking the right solution? *Pacific McGeorge Global Business & Development Law Journal, 26*(2), 285–324.

Segijn, C. M., Strycharz, J., Riegelman, A., & Hennesy, C. (2021). A literature review of personalization transparency and control: Introducing the transparency–awareness–control framework. *Media and Communication, 9*(4), 120–133.

Sekaran, U., & Bougie, R. (2016). *Research methods for business: A skill-building*

approach (7th ed.). John Wiley & Sons.

Sheeran, P., Webb, T. L., & Gollwitzer, P. M. (2005). The interplay between goal intentions and implementation intentions. *Personality and Social Psychology Bulletin, 31*(1), 87–98.

Singh, J. (1991). Redundancy in constructs: Problem, assessment, and an illustrative example. *Journal of Business Research, 22*(3), 255–280.

Smit, E. G., Van Noort, G., & Voorveld, H. A. (2014). Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe. *Computers in Human Behaviour, 32,* 15–22.

Smith, H. (1980). A modest test of cross–cultural differences in sexual modesty, embarrassment and self–disclosure. *Qualitative Sociology, 3*(3), 223–241.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*(4), 989–1015.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly, 20*(2), 167–196.

Speck, P. S., & Elliott, M. T. (1997). Predictors of advertising avoidance in print and broadcast media. *Journal of Advertising, 26*(3), 61–76.

Stanaland, A. J., Lwin, M. O., & Miyazaki, A. D. (2011). Online privacy trustmarks: Enhancing the perceived ethics of digital advertising. *Journal of Advertising Research, 51*(3), 511–523.

Stern, B. B. (2006). What does brand mean? Historical–analysis method and construct

definition. *Journal of the Academy of Marketing Science, 34*(2), 216–223.

Stern, B., Zinkhan, G. M., & Jaju, A. (2001). Marketing images: Construct definition, measurement issues, and theory development. *Marketing Theory, 1*(2), 201–224.

Strycharz, J., & Segijn, C. M. (2022). The future of dataveillance in advertising theory and practice. *Journal of Advertising, 51*(5), 574–591.

Strycharz, J., Van Noort, G., Smit, E., & Helberger, N. (2019). Protective behavior against personalized ads: Motivation to turn personalization off. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 13*(2), Article 1.

Stuart, A., Bandara, A. K., & Levine, M. (2019). The psychology of privacy in the digital age. *Social and Personality Psychology Compass, 13*(11), e12507.

Thierer, A. (2013). The pursuit of privacy in a world where information control is failing. *Harvard Journal of Law & Public Policy, 36*(2), 409–455.

Thorson, A. R. (2015). Investigating adult children's experiences with privacy turbulence following the discovery of parental infidelity. *Journal of Family Communication, 15*(1), 41–57.

Treiblmaier, H., & Pollach, I. (2007). Users' perceptions of benefits and costs of personalization. In *Proceedings of the 28th International Conference on Information Systems (ICIS 2007)* (Paper 141). Association for Information Systems.

Trepte, S. (2021). The social media privacy model: Privacy and communication in the

light of social media affordances. *Communication Theory, 31*(4), 549–570.

Trepte, S., Reinecke, L., Ellison, N. B., Quiring, O., Yao, M. Z., & Ziegele, M. (2017). A cross-cultural perspective on the privacy calculus. *Social Media + Society, 3*(1), Article 2056305116688035.

Turow, J., Carpini, M. X. D., Draper, N. A., & Howard-Williams, R. (2012). *Americans roundly reject tailored political advertising*. Annenberg School for Communication, University of Pennsylvania.

Ur, B., Leon, P. G., Cranor, L. F., Shay, R., & Wang, Y. (2012). Smart, useful, scary, creepy: Perceptions of online behavioral advertising. In *Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS 2012)* (pp. 1–15). Association for Computing Machinery.

Van Doorn, J., & Hoekstra, J. C. (2013). Customization of online advertising: The role of intrusiveness. *Marketing Letters, 24*(4), 339–351.

Van Eijk, N., Helberger, N., Kool, L., van der Plas, A., & van der Sloot, B. (2012). Online tracking: Questioning the power of informed consent. *Info, 14*(5), 57–73.

Van Noort, G., Smit, E. G., & Voorveld, H. A. (2013). The online behavioural advertising icon: Two user studies. In P. De Pelsmacker (Ed.), *Advances in advertising research (Vol. IV): The changing roles of advertising* (pp. 365–378). Springer.

Varnali, K. (2021). Online behavioral advertising: An integrative review. *Journal of Marketing Communications, 27*(1), 93–114.

Walrave, M., Van Ouytsel, J., Ponnet, K., & Temple, J. R. (2018). Sharing and caring? The role of social media and privacy in sexting behaviour. In M. Walrave, J. Van Ouytsel, K. Ponnet, & J. R. Temple (Eds.), *Sexting: Motives and risk in online sexual self-presentation* (pp. 1–17). Palgrave Macmillan.

Watkins, D. C., Wharton, T., Mitchell, J. A., Matusko, N., & Kales, H. C. (2017). Perceptions and receptivity of nonspousal family support: A mixed methods study of psychological distress among older, church–going African American men. *Journal of Mixed Methods Research, 11*(4), 487–509.

Weinstein, W. L. (1971). The private and the free: A conceptual inquiry. In J. R. Pennock & J. W. Chapman (Eds.), *Nomos XIII: Privacy* (pp. 624–692). Atherton Press.

Westin, A. F. (1968). Privacy and freedom. *Washington and Lee Law Review, 25*(1), 166–170.

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

Wohn, D. Y., Solomon, J., Sarkar, D., & Vaniea, K. E. (2015). Factors related to privacy concerns and protection behaviors regarding behavioral advertising. In *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '15)* (pp. 2257–2262). Association for Computing Machinery.

Yang, H. (2013). Young American consumers' online privacy concerns, trust, risk, social media use, and regulatory support. *Journal of New Communications*

Research, 5(1), 1–30.

Yao, Y., Lo Re, D., & Wang, Y. (2017). Folk models of online behavioral advertising. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW '17)* (pp. 1957–1969). Association for Computing Machinery.

Youn, S. (2005). Teenagers' perceptions of online privacy and coping behaviors: a risk–benefit appraisal approach. *Journal of Broadcasting & Electronic Media, 49*(1), 86–110.

Yun, H., Lee, G., & Kim, D. J. (2019). A chronological review of empirical research on personal information privacy concerns: An analysis of contexts and research constructs. *Information & Management, 56*(4), 570–601.

Zarouali, B., Ponnet, K., Walrave, M., & Poels, K. (2017). "Do you like cookies?" Adolescents' skeptical processing of retargeted Facebook ads and the moderating role of privacy concern and a textual debriefing. *Computers in Human Behavior, 69*, 157–165.

Zhu, Y.-Q., & Chang, J.-H. (2016). The key role of relevance in personalized advertisement: Examining its impact on perceptions of privacy invasion, self-awareness, and continuous use intentions. *Computers in Human Behavior, 65*, 442–447.

Zuboff, S. (2019). Surveillance capitalism and the challenge of collective action. *New Labor Forum, 28*(1), 10–29.

Appendix A. Massey Human Ethical Approval

Kia ora,

Link to application
HoU Review Group

Ethics Notification Number: 4000028326
Title: Understand people's privacy as a state in the context of Online Behavioural Advertising.

Thank you for submitting a low risk notification for your research/teaching/evaluation.

This email is to acknowledge receipt of the low risk notification and to inform you that the details of your project have been recorded in our database for inclusion in the annual reports to the Health Research Council Ethics Committee (HRCEC) and the Massey University Research Committee (URC).

You may proceed with your research, though it is advisable to provide a couple of weeks before commencing, as all low risk notifications are checked for completeness and clarity by a Research Ethics Advisor. You may be contacted if your application is incomplete and/or further clarification is required.

The low risk notification for this project is valid for a maximum of three years.

Please notify me if situations subsequently occur which cause you to reconsider your initial ethical analysis.

If a sponsoring organisation, funding authority (e.g., the Health Research Council) or a journal require evidence of ethical approval from a Human Ethics Committee (with an approval number), you need to complete a full Massey University Human Ethics application to bereviewed and approved by one of our Human Ethics Committees. Applications must besubmitted and approved prior to the commencement of the research.

Please note that travel undertaken by students must be approved by the supervisor and the relevant Pro Vice-Chancellor and be in accordance with the Policy and Procedures for Course-Related Student Travel Overseas. In addition, the supervisor must advise the University's Insurance Officer.

Please include the following statement on all public documents (e.g., information sheet, consent form) related to your project:

This project has been evaluated by peer review and judged to be low risk. Consequently, it has not been reviewed by one of the University's Human Ethics Committees. The researcher(s) named above are responsible for the ethical conduct of this research.

If you have any concerns about the ethical conduct of this research that you want to raise with someone other than the researcher(s), please contact Massey University Human Ethics by email: humanethics@massey.ac.nz.

I wish you all the best in your research, teaching or evaluation activities and appreciate your thoughtful consideration of ethics principles and practices.

If you wish to print a copy of this letter:

1. Please login to the RIMS system (https://rme.massey.ac.nz).
2. In the Ethics menu, select Ethics Applications.
3. Using the Advanced option, select Ethics Applications (Area), Application ID (Search On), enter the ethics notification number in the Value area and select Find on the toolbar.
4. With the application in the Results Tab, tick the empty box on the far left of the application and select Reports from the toolbar.
5. Select the "Human Ethics - Low risk notification letter" link, this will open the report viewer.
6. Select the application code from the Report Parameters dropdown and submit. You can then select an export option from the top toolbar (Print, Save).

Ngā mihi nui,

Professor Tracy Riley
Acting Chair, Research Ethics Chairs' Committee and Acting Director, Research Ethics

Appendix B. Interview Participants Consent Form

Understanding people's privacy as a state in the context of Online Behavioral Advertising

PARTICIPANT CONSENT FORM - INDIVIDUAL

I have read, or have had read to me in my first language, and I understand the Information Sheet attached as Appendix I. I have had the details of the study explained to me, any questions I had have been answered to my satisfaction, and I understand that I may ask further questions at any time. I have been given sufficient time to consider whether to participate in this study and I understand participation is voluntary and that I may withdraw from the study at any time.

1. I agree/do not agree to the interview being sound recorded.
2. I agree/do not agree to the interview being image recorded.
3. I wish/do not wish to have my recordings returned to me.
4. I wish/do not wish to have data placed in an official archive.
5. I agree to participate in this study under the conditions set out in the Information Sheet.

Declaration by Participant:

I _____ [print full name]_____ hereby consent to take part in this study.

Signature: _____ Date: _____

Appendix C. Semi-Structured Interview Guide

Introduction

Thank you for supporting my PhD research and agreeing to participate in this interview.

My name is Jiaqi Zhu, and I am currently a PhD candidate at Massey University, New Zealand, supervised by Dr. Mark Avis and Dr. Vishnu Menon. We are a research team working on my PhD research. The Ethical Approval of Massey University has approved our research.

Our research is interviewing you to have a better understanding of your privacy in an advertisement context. There are no right or wrong answers to our questions, and we are interested in your feelings and opinions. Your participation is voluntary (not coercion). Your decision to participate or not participate will not affect the experience you currently receive from the context.

The interview should take approximately 20 minutes, depending on how much information you want to share. A gift will be given to you when the interview finishes to appreciate your help with my doctoral study.

** If you have any further concerns about the interview, please contact my supervisors: Dr. Mark Avis (Massey University, Ph: +64 [redacted], Email: M.Avis@massey.ac.nz), Dr. Vishnu Menon (Massey University, Ph: +64 4 979 3655, Email: v.menon@massey.ac.nz).

Consent and Confidential

With your permission, I would like to audio record the interview because I don't want to miss any of your comments. All responses will be kept confidential. This means that your de-identified interview responses will only be shared with research team members- they are my PhD supervisors: Dr. Mark Avis and Dr. Vishnu Menon, and we will ensure that any information we include in our report does not identify you as the respondent. You may decline to answer any question or stop the interview at any time and for any reason. Are there any questions about what I have just explained?

May I turn on the digital recorder?

Conducting Interview

Then, begin the interview. There are two main processes in the interview:

(1) First, watch process materials.

(2) Second, answer the interview questions.

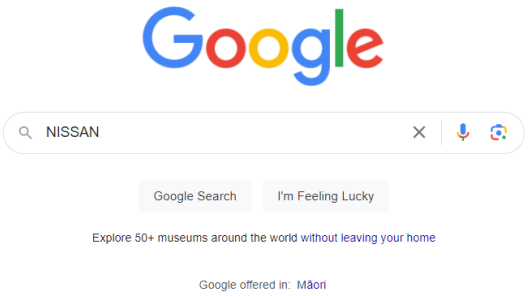
In the first process, you will be provided with an artificial scenario. To help give more ecological results, please imagine you are in the provided scenario as best as possible.

Process Begin

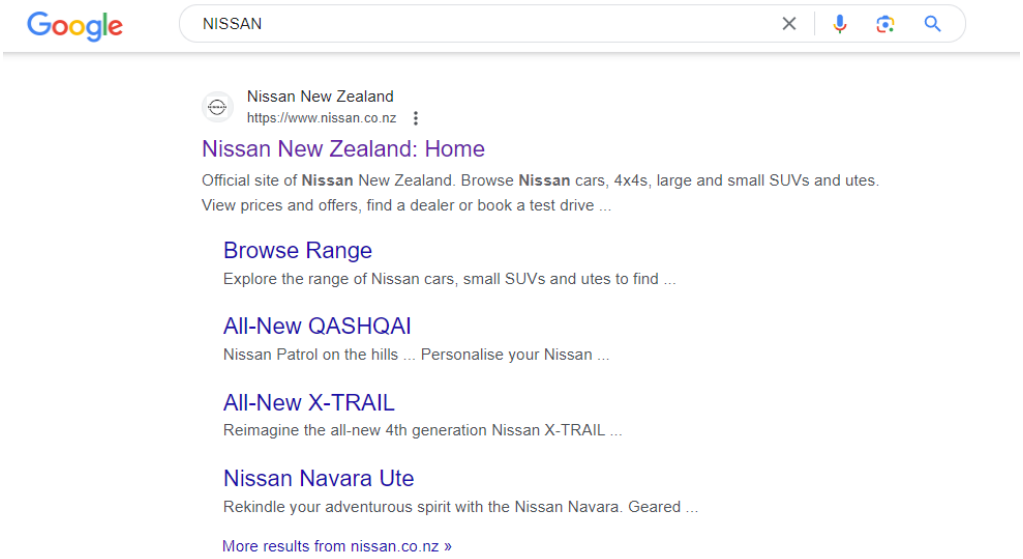
Step 1:

Imagine you want to buy a car and hear from your friends that NISSAN provides high-quality vehicles.

So, you search NISSAN on Google…



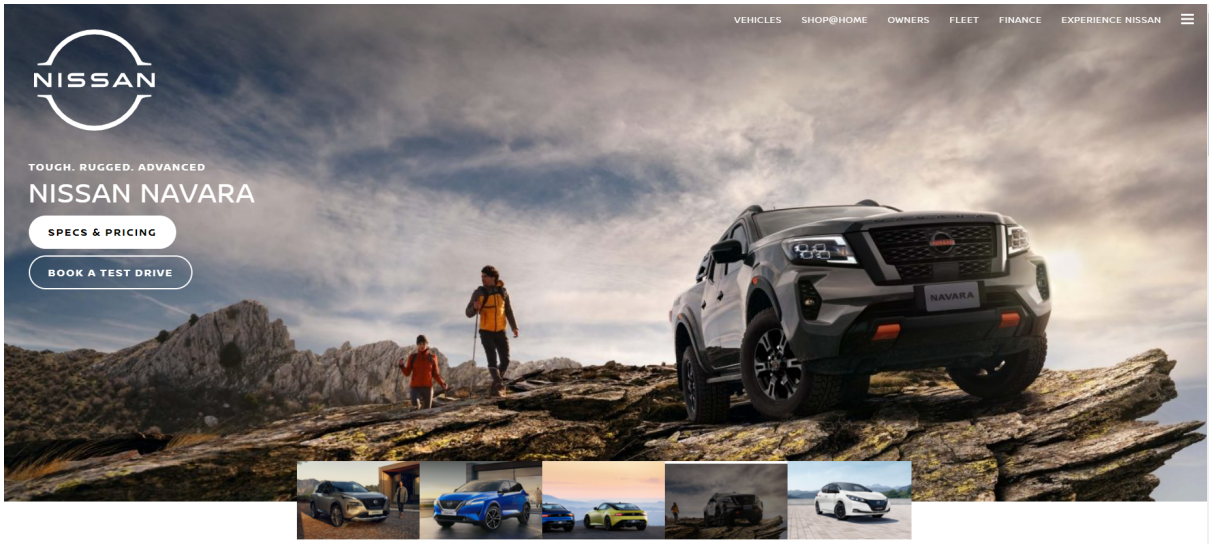
[…] You click the *Nissan New Zealand: Home* (NISSAN's official website) to learn more about the cars.

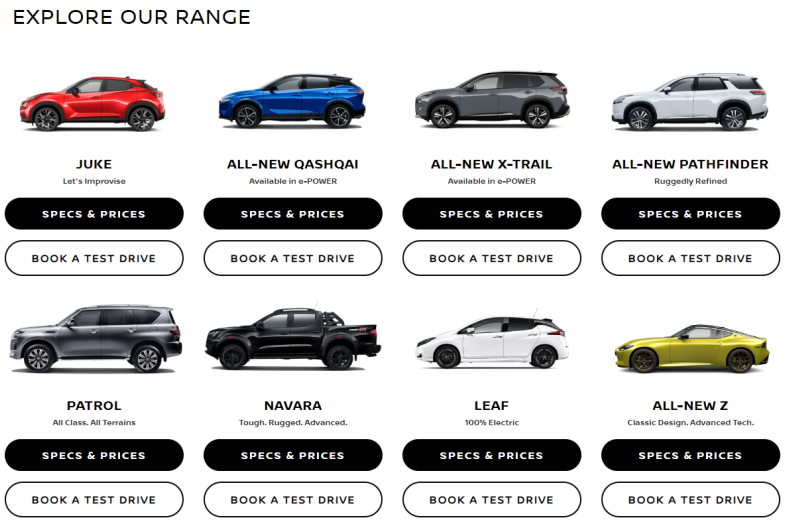

Google
NISSAN
Nissan New Zealand
https://www.nissan.co.nz
Nissan New Zealand: Home
Official site of Nissan New Zealand. Browse Nissan cars, 4x4s, large and small SUVs and utes. View prices and offers, find a dealer or book a test drive ...
Browse Range
Explore the range of Nissan cars, small SUVs and utes to find ...
All-New QASHQAI
Nissan Patrol on the hills ... Personalise your Nissan ...
All-New X-TRAIL
Reimagine the all-new 4th generation Nissan X-TRAIL ...
Nissan Navara Ute
Rekindle your adventurous spirit with the Nissan Navara. Geared ...
More results from nissan.co.nz »

Step 2:

As the fuel price increases, you are considering buying an electric vehicle. You click the 100% Electric NISSAN LEAF.

Nissan website

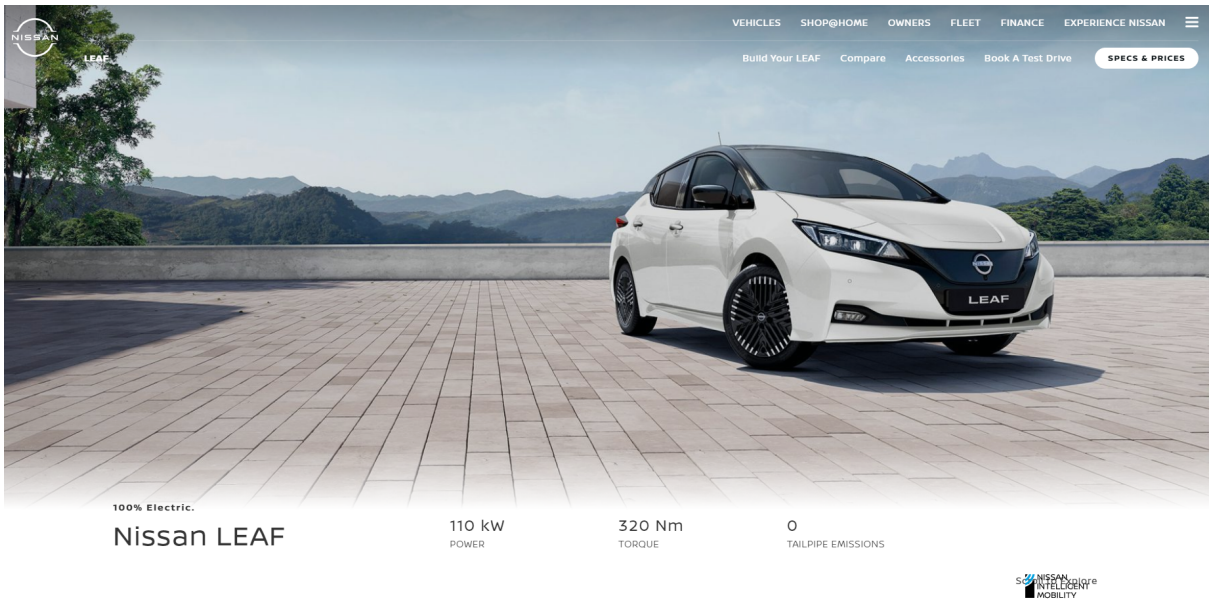




Step 3:

On this website, you view the details of the NISSAN LEAF, including the colour, the appearance, and the price.

Nissan Leaf website



Find your Nissan LEAF

VIEW SPECS & PRICES

LEAF

Driveaway from

$54,990

BUILD YOUR LEAF

- 100% electric motor with zero tailpipe emissions
- 270km indicative driving range*
- 39 kWh battery capacity (usable)
- e-Pedal one pedal driving

COMPARE ALL FEATURES

LEAF e+

Driveaway from

$63,990

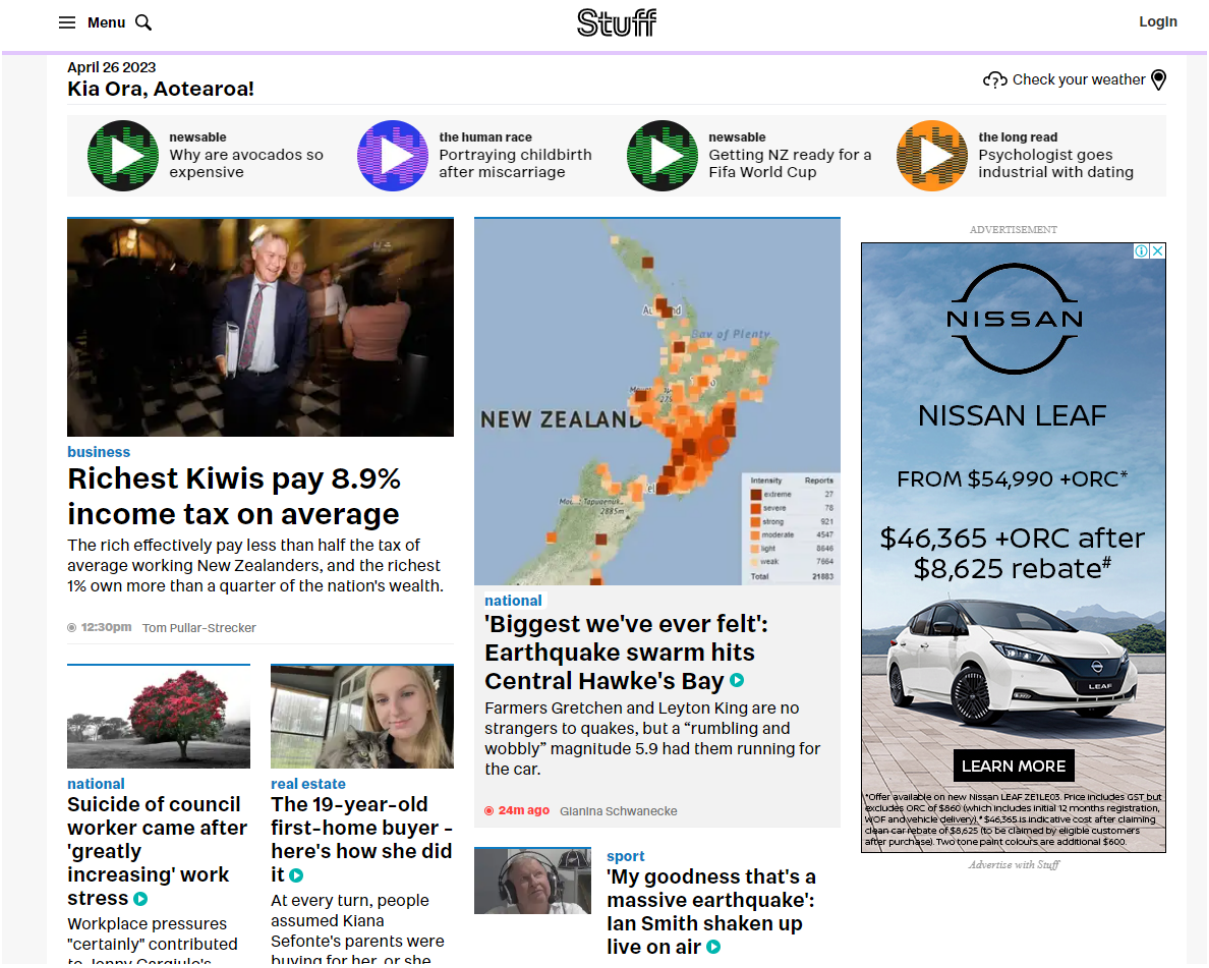
BUILD YOUR LEAF

- 100% electric motor with zero tailpipe emissions
- 59 kWh battery capacity (usable)
- 385km indicative driving range**
- e-Pedal one pedal driving

COMPARE ALL FEATURES

Step 4:

Then, you close the website without purchasing and visit Stuff to watch local news.



Process Finished

In the second process, I will ask you six open questions, and you can answer them based on your experience in the scenario.

1. Screening Question

I want to start asking you some questions now.

Could you tell me whether you have noticed anything related to Nissan Leaf on the Stuff News website?

> **Prompts:** If not, I will tell the participants to do the process again and explain to them that there is a piece of Nissan Leaf advertisement displayed on the Stuff News website.

2. Participants' behaviour intention

Could you please tell me what you do when you watch this ad?

Prompts: Why do you want to take this action?

Now, I'm going to ask you some questions about your knowledge and feelings regarding this context.

3. Participants' privacy state

Could you please tell me your feelings after watching this ad? Please describe to me your feelings.

Prompts: (1) Do you think your privacy has been invaded by this ad? To what extent do you think this ad has invaded your privacy? (2) You mentioned that you had a concern (were concerned/worried) for your privacy. Could you please describe what you mean by concern?

4. Previous Experiences and Knowledge

Have you ever seen this type of advertisement before? How much do you know about this advertisement?

Intervention: show the participant [Intervention Material 1. What is OBA?], and ask:

- Do you think you know more about this ad after watching the video?
- And how do you currently feel? Do you feel more or less [_____ (which you mentioned before)]?
- Besides this feeling, do you have other feelings?

5. Participants' Trade-off

How do you comment on this advertisement?/Do you think this advertisement is useful or not?

What advantages and disadvantages does this commercial can offer you?

Intervention: Show [Intervention Material 2. Benefits and Risks of OBA], and ask:

- What would you like to do on this ad (Note: Need to link to question 2]? What would you do in the future?

6. Conclusion

Is there anything else that you would like to comment on that I haven't already asked you about?

Thank you very much for your time and the information you shared today.

Intervention Materials

Material 1. What is OBA?

I will show you a video by Internet Advertising Bureau (IAB) UK to explain this ad.

Video: How online behavioural advertising works - YouTube

Material 2. Benefits and risks of OBA

Benefits	***Risks***
You could receive interest-based targeted advertisements. So, you will have a personalized, relevant, and efficient Internet browsing experience.	Firms may endlessly know your online activity information (search history, browsing history, click history, etc.).
You may receive cost reductions.	Some ads may foster you to make emotional and unconscious choices.
You could receive special offers and gifts.	Firms may know your identity, financial situation, and physical information if they want.
You may experience faster communication and decision-making process.	You may have feelings of invasiveness.
You may have feelings of being valued by firms.	You may receive increased unsolicited advertisements.

Appendix D. Sample Participant's Transcript

Participant 10

Participants Demographic	
Age (or year of born)	28
Gender	Male
Nationality	European New Zealander
Occupation	Software Developer
Education level	Master
Currently living city and country	Wellington, NZ
How long have you been there?	Live in NZ my entire life, lived in Wellington for around 7 years

Descriptions of state
[uneasy] [unsure] [uncomfortable] [surprised] [catch me off guard]

Descriptions of privacy invasion level	
OBA in the scenario	[an uneasy sort of feeling] [I'll just say no, I say I think]
different ad contents	
different contexts	[more uncomfortable]

Sources of trade-off	
perceived benefits	[a helpful thing because it's able to show you things that you've already been looking into or after] [if it's something I haven't decided yet, it would also be helpful in a way because it's keep reminding me that I need to make a decision if it's something urgent]
perceived risks	[influence decisions in a way] [I'm trying to get convinced to make a decision towards a certain ideology] [it's trying to target me and made me do something]

Descriptions of behaviour
[purchase] [won't click] [ignore] [click because I'm curious] [run ad blocker] [turn off most tracking]

Transcript

Interviewer 0:02

Okay, so my first question here is what's your feelings after watching this advertising?

Participant 10 0:16

I have two feelings towards it. I have a feeling of the advertised like the targeted advertising is like a helpful thing because it's able to show you things that you've already been looking into or after. But then I have an uneasy sort of feeling as well, because it's keeping hold of sort of the data of what you're kind of looking at and can influence decisions in a way. You're gonna feel like unsure. So I don't know if that really answered the question. It took two sides to it.

[a helpful thing because it's able to show you things that you've already been looking into or after] [uneasy] [an uneasy sort of feeling] [influence decisions in a way] [unsure]

Interviewer 0:58

So do you think this kind of advertising is invading your privacy?

Participant 10 1:21

So yes, yes. But I don't think it's is, I'm gonna put this, I'll just say no, I say I think yeah.

[I'll just say no, I say I think]

Interviewer 1:34

And what will you do towards this advertising?

Participant 10 1:53

Me in particular? If I'm looking for a car, it would make me probably died my decision to actually purchase it. Because it's constantly reaffirming, like I'm already looking at it. So it's hosting more advertisements, so it's gonna make me think about it even more.

[purchase]

Interviewer 2:16

And, you know, this advertising is a commercial advertisement, and how will you feel if you receive a targeted political advertisement?

Participant 10 2:47

I feel like I'm getting trying to get a feel more uncomfortable and I feel like if it was political, I feel like I'm trying to get convinced to make a decision towards a certain ideology. Yeah, like, without me even making a decision, like the advertisements trying to make me decide something without thinking.

[more uncomfortable] [I'm trying to get convinced to make a decision towards a certain ideology]

Interviewer 3:09

What will you feel if this advertisement is financial advertising?

Participant 10 3:27

I mean, like when you mean by financial do you mean like, banks or

Interviewer 3:32

Yeah, yeah, bands or mortgage? Yeah. It depends on what you are searching for.

Participant 10 3:43

Just in cases of financial like saving or mortgage.

Interviewer 3:51

Like if you are broking. If you are broken your car and you. You need some money, and you search those kinds of things on Google, and then you didn't make a decision. And then you Google something else and then there is a mortgage those kind of things telling you, Okay, I'm the manager and our product. Our financial product suits you the best. Yeah, what's your feeling?

Participant 10 4:26

I think I'd probably still feel uncomfortable, but it also if it's something I haven't decided yet, it would also be helpful in a way because it's keep reminding me that I need to make a decision if it's something urgent, like a broken car, for example. I don't like that or be saying use this product or whatever. But I like that it would keep reminding me can.

[uncomfortable] [if it's something I haven't decided yet, it would also be helpful in a way because it's keep reminding me that I need to make a decision if it's something urgent]

Interviewer 4:53

I will say that. Whatever the situation you are in, excepting the political context, if the things showed on the advertisement can help you make a decision or I mean, they're helpful, although you feel uncomfortable or uneasy about being checked, and maybe the data will lose. You will have a look at that advertisement or even click that's advertising.

Participant 10 5:37

me myself. Yeah. I probably won't click on it purely because I know it's trying to target me and made me do something. I kind of learned to ignore it in a way because I know it's tracked my data. I know what happens with my data. And I was just trying to what's the word convinced me to do something based off what I've been searching or what I've been talking to with people about. And it can be anything important. So I tried to ignore it.

[won't click] [it's trying to target me and made me do something] [ignore]

But sometimes something will pop up. Yeah, I'll be surprised and it will catch me off guard. There have been cases where I have been searching something up and it will pop up. Pop up it will show some advertisement or something I've never heard of before. And I will click on it just because I'm curious. Maybe it hasn't shown up on Google before. So there's some small cases where it is helpful. It's another way of searching things but a lot of it seems to I notice it's like the big sponsors or big companies that will just show up most of the time.

[surprised] [catch me off guard] [click because I'm curious]

Interviewer 6:56

Okay. And will you also do any protection behavior like changing your privacy setting on the Google or report those advertisements to the Google or using some ad blocking things?

Participant 10 7:16

I always run an ad blocker, And I have run out a browser which has a built in VPN into it. So my data normally doesn't get tracked as much but you can't stop with everything. Like it's harder to stop that with your phones unless you pay for a VPN. And I try to turn off most tracking like all tracking on my phone as well. Trying to mitigate it.

[run ad blocker] [turn off most tracking]

Interviewer 7:44

Sure. That's all of the interview. And thanks for your support. Thanks for your opinion.

Appendix E. Massey Human Ethical Approval

Kia ora,

Link to Application
HoU Review Group

Ethics Notification Number: 4000029284
Title: Is consumers' privacy as a state generalisable to every context?

Thank you for submitting a low risk notification for your research/teaching/evaluation.

This email is to acknowledge receipt of the low risk notification and to inform you that the details of your project have been recorded in our database for inclusion in the annual reports to the Health Research Council Ethics Committee (HRCEC) and the Massey University Research Committee (URC).

You may proceed with your research, though it is advisable to provide a couple of weeks before commencing, as all low risk notifications are checked for completeness and clarity by a Research Ethics Advisor. You may be contacted if your application is incomplete and/or further clarification is required.

The low risk notification for this project is valid for a maximum of three years.

Please notify me if situations subsequently occur which cause you to reconsider your initial ethical analysis.

If a sponsoring organisation, funding authority (e.g., the Health Research Council) or a journal require evidence of ethical approval from a Human Ethics Committee (with an approval number), you need to complete a full Massey University Human Ethics application to be reviewed and approved by one of our Human Ethics Committees. Applications must be submitted and approved prior to the commencement of the research.

Please note that travel undertaken by students must be approved by the supervisor and the relevant Pro Vice-Chancellor and be in accordance with the Policy and Procedures for Course-Related Student Travel Overseas. In addition, the supervisor must advise the University's Insurance Officer.

Please include the following statement on all public documents (e.g., information sheet, consent form) related to your project:

This project has been evaluated by peer review and judged to be low risk. Consequently, it has not been reviewed by one of the University's Human Ethics Committees. The researcher(s) named above are responsible for the ethical conduct of this research.

If you have any concerns about the ethical conduct of this research that you want to raise with someone other than the researcher(s), please contact Massey University HumanEthics by email: humanethics@massey.ac.nz.

I wish you all the best in your research, teaching or evaluation activities and appreciate your thoughtful consideration of ethics principles and practices.

If you wish to print a copy of this letter:

1. Please login to the RIMS system (https://rme.massey.ac.nz).
2. In the Ethics menu, select Ethics Applications.
3. Using the Advanced option, select Ethics Applications (Area), Application ID (Search On), enter the ethics notification number in the Value area and select Find on the toolbar.
4. With the application in the Results Tab, tick the empty box on the far left of the application and select Reports from the toolbar.
5. Select the "Human Ethics - Low risk notification letter" link, this will open the report viewer.
6. Select the application code from the Report Parameters dropdown and submit. You can then select an export option from the top toolbar (Print, Save).

Ngā mihi nui,

Professor Tracy Riley
Acting Chair, Research Ethics Chairs' Committee

Appendix F. Online Questionnaire

Hi.

You are invited to participate in a 15-minute anonymous online survey about your feelings in three scenarios that simulate day-to-day situations. In addition to asking some questions about the scenarios, we will also ask for some demographic information.

This survey has been evaluated and judged to be low risk under the Massey University ethics system. The data you provide is anonymous and will be kept confidential. Your data in this online survey will only be used for research purposes by research team members. You may decline to answer any question or stop the interview at any time and for any reason.

The researcher named below is responsible for the ethical conduct of this research. Miss Jiaqi Zhu (Massey University, Ph:+64 [redacted], Email: jzhu5@massey.ac.nz

If you have any concerns about the conduct of this research that you want to raise with someone other than the researcher(s), please contact Dr Brian Finch, Director - Ethics, telephone 06 3569099 ext 86015, email humanethics@massey.ac.nz. “

□ Yes, I consent.

□ No, I do not consent.

SCENARIO 1

Imagine that when you are shopping online, you view a book. And then, you decide to visit another website to book your flight tickets for your holiday. While on the ticket booking website, you receive an advertisement which shows the book that you viewed.

1. What are your potential feelings in this scenario? Please tick any feeling you may experience in the following list.

Creepy □	Angry □
Afraid □	Uneasy □
Scary □	Concerned □
Hopeless □	Surprised □
Dangerous □	Monitored □
Risky □	Manipulated □
Informative □	Lonely □
Threatened □	Violated □
Offended □	Insecure □
Sad □	Excited □
Peaceful □	Happy □
Annoyed □	Dislike □
Embarrassed □	Uncomfortable □

2. Please write down any additional feelings you have that are not listed above _____.

3. Are you aware that online advertising uses systems to track your online behaviour?

□ Yes, I am.

□ No, I am not.

SCENARIO 2

You are going swimming at a new swimming pool for the first time. You enter the changing room for the swimming pool and several people are getting changed. You look around and notice there are no cubicles and it is open-plan. The only place to change into your bathing costume is in this changing room.

1. What are your potential feelings in this scenario? Please tick any feeling you may experience in the following list.

Creepy □	Angry □
Afraid □	Uneasy □
Scary □	Concerned □
Hopeless □	Surprised □
Dangerous □	Monitored □
Risky □	Manipulated □
Informative □	Lonely □
Threatened □	Violated □
Offended □	Insecure □
Sad □	Excited □
Peaceful □	Happy □
Annoyed □	Dislike □
Embarrassed □	Uncomfortable □

2. Please write down any additional feelings you have that are not listed above _____.

3. Have you experienced this or an equivalent situation before?

□ Yes, I have.

□ No, I have not.

SCENARIO 3

Imagine that you have a particularly challenging day at work and confide in your partner (girlfriend or boyfriend) about a conflict you had with your boss. You express your frustrations and fears about your job security. Your partner shares your story with his friends during a casual evening gathering, mentioning your struggles at work and hoping to get some advice or support for you.

1. What are your potential feelings in this scenario? Please tick any feeling you may experience in the following list.

Creepy □	Angry □
Afraid □	Uneasy □
Scary □	Concerned □
Hopeless □	Surprised □
Dangerous □	Monitored □
Risky □	Manipulated □
Informative □	Lonely □
Threatened □	Violated □
Offended □	Insecure □
Sad □	Excited □
Peaceful □	Happy □
Annoyed □	Dislike □
Embarrassed □	Uncomfortable □

2. Please write down any additional feelings you have that are not listed above _____.

3. Are you currently in a relationship?

□ Yes, I am.

□ No, I am not.

(If Yes) How long have you been in this relationship?

□ less than 1 year

□ 1-3 years

□ 3-5 years

□ over 5 years

Now, we invite you to provide some basic information about yourself. Please note that this is anonymous.

1. What is your gender?
   - □ Female
   - □ Male
   - □ I prefer not to say
2. What is your age? _____
3. What is your education level?
   - □ School
   - □ Tertiary
   - □ Bachelor
   - □ Master
   - □ PhD
4. What is your nationality? _____
5. Which country's culture do you most identify with? _____

In the end of the survey, please finish the seven-point Likert scale with 1 ("strongly disagree") to 7 ("strongly agree") It is very important to me to feel that I can choose what others get to know about me.

1. It is very important to me to be able to choose who gets to see my personal information or not.
2. It is very important to be able to keep some things to myself.
3. It is very important to me that records pertaining to me are kept confidential.
4. Generally, there is not much I am willing to share with those who are not family or close acquaintances.

END OF THE SURVEY

Appendix G. Binary Logistic Regression Results

Table G1. *Binary logistic regression predicting likelihood of feeling "creepy" across contexts, controlling for demographic variables*

(Reference categories: Context = Interpersonal; Region = NZ; Gender = Prefer not to say; Age group = above 60; Education = PhD) Note. Reference groups are marked in parentheses. OR = Odds Ratio. CI = Confidence Interval. Model $\chi^2(14) = 278.60$, $p < .001$; Nagelkerke $R^2 = .207$.

Predictor	B	S.E.	Wald	p	OR	95% CI for OR
Context			96.09	<.001		
OBA (vs Interpersonal)	-0.793	0.142	31.42	<.001	0.452	[0.343, 0.597]
CR (vs Interpersonal)	-1.607	0.169	90.51	<.001	0.200	[0.144, 0.279]
Age Group			23.88	<.001		
Under 18 (vs 60+)	-0.495	0.262	3.58	.059	0.609	[0.365, 1.018]
18–29 (vs 60+)	-0.603	0.193	9.79	.002	0.547	[0.375, 0.798]
30–44 (vs 60+)	-0.373	0.205	3.32	.069	0.689	[0.461, 1.029]
45–60 (vs 60+)	-1.433	0.317	20.41	<.001	0.239	[0.128, 0.444]
Region			126.43	<.001		
US (vs NZ)	-1.807	0.164	121.05	<.001	0.164	[0.119, 0.227]
China (vs NZ)	-2.021	0.290	48.50	<.001	0.132	[0.075, 0.234]
Gender			1.41	.495		
Female (vs Prefer not)	0.159	0.136	1.37	.241	1.172	[0.898, 1.530]
Male (vs Prefer not)	0.037	0.212	0.03	.860	1.038	[0.685, 1.572]
Education			13.99	.007		
School (vs PhD)	0.377	0.246	2.35	.125	1.457	[0.900, 2.359]
Tertiary (vs PhD)	0.101	0.170	0.35	.552	1.107	[0.793, 1.544]
Bachelor (vs PhD)	-0.556	0.264	4.45	.035	0.573	[0.342, 0.961]
Master (vs PhD)	0.395	0.230	2.97	.085	1.485	[0.947, 2.329]
Constant	0.711	0.248	8.20	.004	2.036	—

Table G2. *Binary logistic regression predicting likelihood of feeling "scary" across contexts, controlling for demographic variables*

(Reference categories: Context = Interpersonal; Region = NZ; Gender = Prefer not to say; Age group = above 60; Education = PhD) Note. Reference groups are marked in parentheses. OR = Odds Ratio. CI = Confidence Interval. Model $\chi^2(14) = 108.176$, $p < .001$; Nagelkerke $R^2 = .125$.

Predictor	B	S.E.	Wald	p	OR	95% CI for OR
Context			12.99	.002		
OBA (vs Interpersonal)	-0.425	0.203	4.37	.036	0.654	[0.439, 0.974]
CR (vs Interpersonal)	-0.780	0.222	12.37	<.001	0.459	[0.297, 0.708]
Age Group			12.44	.014		
Under 18 (vs 60+)	0.439	0.371	1.40	.237	1.552	[0.750, 3.212]
18–29 (vs 60+)	0.377	0.294	1.65	.199	1.457	[0.820, 2.591]
30–44 (vs 60+)	0.136	0.322	0.18	.673	1.145	[0.609, 2.153]
45–60 (vs 60+)	-0.960	0.485	3.92	.048	0.383	[0.148, 0.991]
Region			45.49	<.001		
US (vs NZ)	-1.491	0.224	44.15	<.001	0.225	[0.145, 0.350]
China (vs NZ)	-1.536	0.422	13.22	<.001	0.215	[0.094, 0.493]
Education			22.38	<.001		
School (vs PhD)	-0.773	0.435	3.16	.076	0.461	[0.197, 1.083]
Tertiary (vs PhD)	-0.509	0.249	4.17	.041	0.601	[0.369, 0.980]
Bachelor (vs PhD)	0.029	0.311	0.01	.926	1.029	[0.560, 1.892]
Master (vs PhD)	0.693	0.275	6.35	.012	1.999	[1.166, 3.428]
Gender			3.09	.213		
Female (vs Prefer not)	0.324	0.193	2.81	.093	1.383	[0.947, 2.018]
Male (vs Prefer not)	0.309	0.303	1.04	.307	1.362	[0.753, 2.465]
Constant	-1.447	0.372	15.11	<.001	0.235	—

Table G3. *Binary logistic regression predicting likelihood of feeling "annoyed" across contexts, controlling for demographic variables*

(Reference categories: Context = Interpersonal; Region = NZ; Gender = Prefer not to say; Age group = above 60; Education = PhD) Note. Reference groups are marked in parentheses. OR = Odds Ratio. CI = Confidence Interval. Model $\chi^2(14) = 288.76$, $p < .001$; Nagelkerke $R^2 = .228$.

Predictor	B	S.E.	Wald	p	OR	95% CI for OR
Context			25.30	<.001		
OBA (vs Interpersonal)	0.138	0.175	0.62	.431	1.148	[0.814, 1.618]
CR (vs Interpersonal)	0.753	0.165	20.90	<.001	2.124	[1.538, 2.933]
Age Group			16.22	.003		
Under 18 (vs 60+)	0.387	0.311	1.55	.214	1.472	[0.800, 2.708]
18–29 (vs 60+)	0.621	0.248	6.27	.012	1.861	[1.144, 3.028]
30–44 (vs 60+)	0.339	0.268	1.60	.206	1.404	[0.830, 2.376]
45–60 (vs 60+)	1.082	0.324	11.16	<.001	2.951	[1.564, 5.570]
Region			122.16	<.001		
US (vs NZ)	-1.941	0.176	122.15	<.001	0.144	[0.102, 0.203]
China (vs NZ)	-1.334	0.288	21.43	<.001	0.263	[0.150, 0.463]
Gender			1.16	.559		
Female (vs Prefer not)	-0.057	0.149	0.15	.702	0.945	[0.706, 1.264]
Male (vs Prefer not)	0.205	0.235	0.76	.384	1.227	[0.774, 1.946]
Education			3.45	.485		
School (vs PhD)	-0.136	0.293	0.22	.642	0.872	[0.491, 1.550]
Tertiary (vs PhD)	0.029	0.183	0.03	.874	1.029	[0.719, 1.473]
Bachelor (vs PhD)	-0.078	0.247	0.10	.753	0.925	[0.570, 1.500]
Master (vs PhD)	0.361	0.246	2.15	.142	1.434	[0.886, 2.323]
Constant	-1.390	0.308	20.37	<.001	0.249	—

Table G4 *Binary logistic regression predicting likelihood of feeling "uneasy" across contexts, controlling for demographic variables*

(Reference categories: Context = Interpersonal; Region = NZ; Gender = Prefer not to say; Age group = above 60; Education = PhD) Note. Reference groups are marked in parentheses. OR = Odds Ratio. CI = Confidence Interval. Model $\chi^2(14) = 148.560$, $p < .001$; Nagelkerke $R^2 = .120$.

Predictor	B	S.E.	Wald	p	OR	95% CI for OR
Context			25.62	<.001		
OBA (vs Interpersonal)	0.592	0.152	15.23	<.001	1.808	[1.343, 2.435]
CR (vs Interpersonal)	-0.112	0.167	0.45	.504	0.894	[0.645, 1.241]
Age Group			23.79	<.001		
Under 18 (vs 60+)	0.470	0.277	2.88	.090	1.599	[0.930, 2.751]
18–29 (vs 60+)	0.397	0.218	3.30	.069	1.487	[0.969, 2.280]
30–44 (vs 60+)	0.229	0.237	0.93	.334	1.258	[0.790, 2.003]
45–60 (vs 60+)	1.306	0.305	18.33	<.001	3.690	[2.030, 6.707]
Region			25.48	<.001		
US (vs NZ)	-0.817	0.165	24.41	<.001	0.442	[0.319, 0.611]
China (vs NZ)	-0.890	0.296	9.07	.003	0.411	[0.230, 0.733]
Education Level			9.61	.048		
School (vs PhD)	0.210	0.269	0.61	.437	1.233	[0.727, 2.091]
Tertiary (vs PhD)	0.404	0.171	5.58	.018	1.498	[1.071, 2.094]
Bachelor (vs PhD)	0.294	0.242	1.48	.224	1.342	[0.835, 2.157]
Master (vs PhD)	0.645	0.231	7.81	.005	1.906	[1.212, 2.997]
Gender			3.29	.193		
Female (vs Prefer not)	-0.182	0.143	1.63	.202	0.833	[0.630, 1.103]
Male (vs Prefer not)	0.196	0.214	0.84	.359	1.216	[0.800, 1.849]
Constant	-1.896	0.281	45.67	<.001	0.150	—

Table G5. *Binary logistic regression predicting likelihood of feeling "monitored" across contexts, controlling for demographic variables*

(Reference categories: Context = Interpersonal; Region = NZ; Gender = Prefer not to say; Age group = above 60; Education = PhD) Note. Reference groups are marked in parentheses. OR = Odds Ratio. CI = Confidence Interval. Model $\chi^2(14) = 226.75$, $p < .001$; Nagelkerke $R^2 = .193$.

Predictor	B	S.E.	Wald	p	OR	95% CI for OR
Context			146.51	<.001		
OBA (vs Interpersonal)	-1.275	0.157	65.58	<.001	0.279	[0.205, 0.380]
CR (vs Interpersonal)	-2.553	0.244	109.28	<.001	0.078	[0.048, 0.126]
Age Group			6.53	0.163		
Under 18 (vs 60+)	0.165	0.299	0.31	0.581	1.180	[0.656, 2.122]
18–29 (vs 60+)	0.291	0.211	1.89	0.169	1.337	[0.884, 2.023]
30–44 (vs 60+)	-0.046	0.239	0.04	0.846	0.955	[0.597, 1.526]
45–60 (vs 60+)	0.548	0.352	2.43	0.119	1.729	[0.868, 3.444]
Region			9.70	0.008		
US (vs NZ)	-0.387	0.193	4.01	0.045	0.679	[0.465, 0.992]
China (vs NZ)	-1.093	0.361	9.16	0.002	0.335	[0.165, 0.680]
Gender			15.62	<.001		
Female (vs Prefer not)	-0.574	0.164	12.24	<.001	0.563	[0.408, 0.777]
Male (vs Prefer not)	0.200	0.215	0.87	0.352	1.222	[0.802, 1.862]
Education			0.60	0.963		
School (vs PhD)	0.146	0.283	0.26	0.607	1.157	[0.664, 2.015]
Tertiary (vs PhD)	0.124	0.182	0.46	0.496	1.132	[0.792, 1.619]
Bachelor (vs PhD)	0.140	0.275	0.26	0.609	1.151	[0.672, 1.971]
Master (vs PhD)	0.078	0.272	0.08	0.776	1.081	[0.634, 1.842]
Constant	-0.708	0.282	6.33	0.012	0.492	—

Table G6. *Binary logistic regression predicting likelihood of feeling "dislike" across contexts, controlling for demographic variables*

(Reference categories: Context = Interpersonal; Region = NZ; Gender = Prefer not to say; Age group = above 60; Education = PhD) Note. Reference groups are marked in parentheses. OR = Odds Ratio. CI = Confidence Interval. Model $\chi^2(14) = 54.58$, $p < .001$; Nagelkerke $R^2 = .042$

Predictor	B	S.E.	Wald	p	OR	95% CI for OR
Context			17.74	<.001		
OBA (vs Interpersonal)	0.361	0.147	6.06	.014	1.434	[1.076, 1.911]
CR (vs Interpersonal)	0.600	0.142	17.73	<.001	1.822	[1.378, 2.409]
Age Group			1.69	.793		
Under 18 (vs 60+)	0.217	0.240	0.81	.367	1.242	[0.775, 1.990]
18–29 (vs 60+)	0.186	0.172	1.17	.279	1.204	[0.860, 1.686]
30–44 (vs 60+)	0.204	0.190	1.16	.282	1.227	[0.845, 1.780]
45–60 (vs 60+)	0.319	0.310	1.06	.303	1.376	[0.749, 2.529]
Region			1.25	.535		
US (vs NZ)	-0.059	0.163	0.13	.716	0.942	[0.685, 1.297]
China (vs NZ)	-0.289	0.265	1.19	.275	0.749	[0.446, 1.258]
Gender			27.67	<.001		
Female (vs Prefer not)	-0.626	0.136	21.12	<.001	0.535	[0.410, 0.698]
Male (vs Prefer not)	0.229	0.172	1.77	.183	1.258	[0.897, 1.763]
Education			3.10	.541		
School (vs PhD)	0.231	0.231	1.00	.318	1.260	[0.801, 1.983]
Tertiary (vs PhD)	0.107	0.149	0.51	.474	1.113	[0.831, 1.490]
Bachelor (vs PhD)	0.081	0.237	0.12	.733	1.084	[0.681, 1.727]
Master (vs PhD)	0.347	0.215	2.61	.106	1.415	[0.929, 2.156]
Constant	-1.803	0.245	53.91	<.001	0.165	—

Table G7. *Binary logistic regression predicting likelihood of feeling "risky" across contexts, controlling for demographic variables*

(Reference categories: Context = Interpersonal; Region = NZ; Gender = Prefer not to say; Age group = above 60; Education = PhD) Note. Reference groups are marked in parentheses. OR = Odds Ratio. CI = Confidence Interval. Model $\chi^2(14) = 127.73$, $p < .001$; Nagelkerke $R^2 = .107$

Predictor	B	S.E.	Wald	p	OR	95% CI for OR
Context			80.05	<.001		
OBA (vs Interpersonal)	-0.916	0.151	36.96	<.001	0.400	[0.298, 0.538]
CR (vs Interpersonal)	-1.401	0.172	66.67	<.001	0.246	[0.176, 0.345]
Age Group			15.09	.005		
Under 18 (vs 60+)	0.788	0.262	9.04	.003	2.199	[1.316, 3.675]
18–29 (vs 60+)	0.342	0.197	3.00	.083	1.408	[0.956, 2.072]
30–44 (vs 60+)	0.335	0.216	2.41	.121	1.398	[0.916, 2.134]
45–60 (vs 60+)	-0.415	0.385	1.16	.281	0.660	[0.311, 1.404]
Region			18.50	<.001		
US (vs NZ)	-0.642	0.173	13.78	<.001	0.526	[0.375, 0.739]
China (vs NZ)	-1.113	0.309	12.98	<.001	0.329	[0.179, 0.602]
Gender			4.80	.091		
Female (vs Prefer not)	-0.031	0.147	0.04	.835	0.970	[0.727, 1.294]
Male (vs Prefer not)	0.401	0.199	4.08	.044	1.494	[1.012, 2.206]
Education			14.24	.007		
School (vs PhD)	-0.174	0.262	0.44	.507	0.841	[0.503, 1.404]
Tertiary (vs PhD)	-0.249	0.169	2.18	.140	0.779	[0.560, 1.085]
Bachelor (vs PhD)	-1.096	0.316	12.03	<.001	0.334	[0.180, 0.621]
Master (vs PhD)	0.106	0.236	0.20	.652	1.112	[0.701, 1.765]
Constant	-0.779	0.262	8.85	.003	0.459	—

Table G8. *Binary logistic regression predicting likelihood of feeling "manipulated" across contexts, controlling for demographic variables*

(Reference categories: Context = Interpersonal; Region = NZ; Gender = Prefer not to say; Age group = above 60; Education = PhD) Note. Reference groups are marked in parentheses. OR = Odds Ratio. CI = Confidence Interval. Model $\chi^2(14) = 134.64$, $p < .001$; Nagelkerke $R^2 = .159$

Predictor	B	S.E.	Wald	p	OR	95% CI for OR
Context			81.83	<.001		
OBA (vs Interpersonal)	-1.919	0.265	52.54	<.001	0.147	[0.087, 0.247]
CR (vs Interpersonal)	-1.575	0.233	45.56	<.001	0.207	[0.131, 0.327]
Age Group			3.74	.443		
Under 18 (vs 60+)	0.143	0.410	0.12	.728	1.153	[0.517, 2.574]
18–29 (vs 60+)	0.314	0.296	1.12	.289	1.369	[0.766, 2.446]
30–44 (vs 60+)	0.428	0.319	1.80	.179	1.534	[0.821, 2.865]
45–60 (vs 60+)	0.763	0.438	3.04	.081	2.145	[0.910, 5.060]
Region			8.55	.014		
US (vs NZ)	-0.543	0.236	5.27	.022	0.581	[0.366, 0.924]
China (vs NZ)	-1.305	0.516	6.39	.011	0.271	[0.099, 0.746]
Education			8.13	.087		
School (vs PhD)	0.603	0.339	3.17	.075	1.827	[0.941, 3.548]
Tertiary (vs PhD)	0.230	0.244	0.89	.346	1.258	[0.781, 2.028]
Bachelor (vs PhD)	0.131	0.365	0.13	.720	1.140	[0.557, 2.330]
Master (vs PhD)	0.778	0.311	6.26	.012	2.178	[1.184, 4.007]
Gender			13.62	.001		
Female (vs Prefer not)	-0.185	0.208	0.79	.375	0.831	[0.552, 1.251]
Male (vs Prefer not)	0.817	0.260	9.87	.002	2.263	[1.360, 3.767]
Constant	-1.891	0.375	25.41	<.001	0.151	—

Table G9. *Binary logistic regression predicting likelihood of feeling "insecure" across contexts, controlling for demographic variables*

(Reference categories: Context = Interpersonal; Region = NZ; Gender = Prefer not to say; Age group = above 60; Education = PhD) Note. Reference groups are marked in parentheses. OR = Odds Ratio. CI = Confidence Interval. Model $\chi^2(14) = 75.63$, $p < .001$; Nagelkerke $R^2 = .061$

Predictor	B	S.E.	Wald	p	OR	95% CI for OR
Context			40.65	<.001		
OBA (vs Interpersonal)	-0.064	0.135	0.22	.637	0.938	[0.720, 1.222]
CR (vs Interpersonal)	-0.979	0.163	36.02	<.001	0.376	[0.273, 0.517]
Age Group			16.86	.002		
Under 18 (vs 60+)	0.060	0.268	0.05	.824	1.061	[0.628, 1.794]
18–29 (vs 60+)	0.486	0.180	7.27	.007	1.626	[1.142, 2.316]
30–44 (vs 60+)	0.081	0.206	0.15	.694	1.085	[0.724, 1.625]
45–60 (vs 60+)	0.820	0.312	6.90	.009	2.271	[1.231, 4.187]
Region			0.73	.694		
US (vs NZ)	0.045	0.175	0.07	.795	1.046	[0.743, 1.475]
China (vs NZ)	-0.156	0.280	0.31	.579	0.856	[0.494, 1.483]
Education			4.14	.387		
School (vs PhD)	0.074	0.249	0.09	.768	1.076	[0.660, 1.755]
Tertiary (vs PhD)	0.186	0.156	1.42	.233	1.205	[0.887, 1.636]
Bachelor (vs PhD)	-0.179	0.261	0.47	.494	0.836	[0.501, 1.396]
Master (vs PhD)	0.290	0.225	1.66	.198	1.336	[0.860, 2.075]
Gender			7.66	.022		
Female (vs Prefer not)	-0.118	0.139	0.71	.398	0.889	[0.677, 1.168]
Male (vs Prefer not)	0.420	0.184	5.21	.022	1.522	[1.061, 2.182]
Constant	-1.694	0.257	43.59	<.001	0.184	—