Doing Privacy Right Or Doing Privacy Rights

Examining The Influence Of Privacy Activities In The Nonmarket Environment On Consumer Attitudes And Intentions.

Valerie Lyons, M.Sc., B.Sc.

Research Supervisors:

Professor Theo Lynn, Dr. Lisa van der Werff, Dr. Grace Fox.

A Thesis submitted to Dublin City University Business School, in partial fulfilment of the requirements for the degree of Doctor of Philosophy

January 2022

DECLARATION

I hereby certify that this material, which I now submit for assessment on the programme of study leading to the award of Doctor of Philosophy is entirely my own work, and that I have exercised reasonable care to ensure that the work is original, and does not to the best of my knowledge breach any law of copyright, and has not been taken from the work of others save and to the extent that such work has been cited and acknowledged within the text of my work.

Signed: ID No.: **16210286**

Date: 26th January 2022

DEDICATION

To my amazing children, my inspirational parents, my wonderful partner, my patient friends and my supportive colleagues

ACKNOWLEDGEMENTS

I wish to express my sincere gratitude to my supervisors, Professor Theo Lynn and Dr. Lisa van der Werff, for their continual support and guidance over the past six years. I feel privileged to have had such great supervisors to help me on this journey. Together they have invested a huge amount of their time in getting both me, and this PhD, across the line. Their expertise has helped sculpt and shape the PhD along its journey, and provided me with great clarity at crucial points of that journey. The PhD would simply not have been possible without them guiding, mentoring, critiquing, and nudging me along the way. Both Theo's and Lisa's positivity, motivation, and belief, encouraged me to persevere throughout this journey. I cannot thank them enough for their valued advice, their honest critiques, the many forms, papers and applications they have revised and completed over the years. I am also indebted to their incredible patience and kindness over some difficult periods during those six years. I am also very thankful to my panel members Dr. Grace Kenny-Fox and Professor Finian Buckley. Grace was a constant source of pragmatic solutions to issues encountered, and a huge source of valued expertise. Finian contributed much sage advice on coping with critical feedback and much positivity and support during progression meetings over the years. I am also grateful to all the academic and administrative staff at Dublin City University who offered support, advice, and encouragement throughout the journey, particularly to Jonny Hobson, who was always tasked with responding to my many administrative questions. I would also like to thank Brian Honan, CEO of BH Consulting, colleague, confidant and friend - for his belief in me, and his support for this PhD, in particular for the significant amount of time off I needed to complete the writeup stage of the PhD.

To my parents, although no longer here, I am so grateful for the love that both showed me and the respect for continuous learning that they instilled in me. I know they would both be

so proud of me, just as they were when I achieved my undergraduate degree and my masters. Not a day goes by where I don't miss them both. To my Dad in particular, who was here when I started this journey - I know you would love to have been around to see me finish it. To my children Dan and Ciara - our lives have taken such a strange journey since December 2016, and doing this PhD has enabled us to spend more time together while we adjusted to our new worlds. This last year, during the pandemic, has been unprecedented - me in my home office working on my PhD and you both upstairs at school. But we did it, we got through it. Hopefully now you both can understand how much time and effort is required for any academic achievement, and can leverage that learning for your own futures. And finally to my wonderful partner, Todd. Thank you for your constant belief in me, unwavering support, endless encouragement, and the many bunches of flowers at various milestones.

This PhD was supported by the Irish Research Council's Postgraduate Employment Based Scheme. Without this scholarship, the PhD would have been far more difficult, so I am grateful to everyone involved in the application for the scholarship and to the Irish Research Council for its provision. I am thankful to the Graduate Studies Office for all their support and help throughout the course of the PhD. I cannot ignore that the last eighteen months of the PhD was conducted during the pandemic, with its lockdowns, working from home, schooling from home and many other 'challenges' the pandemic presented. Thus, I am very grateful to DCU as an academic organisation for the support and guidance provided by all departments throughout the pandemic, the online classes, the financial support and grants, the IT online support and the many wellbeing courses run during this time, many of which I availed of.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

ACQ = Attention Check Question

AMT = Amazon Mechanical Turk

ANOVA = Analysis of Variance

ANCOVA = Analysis of Covariance

AI = Artificial Intelligence

CCPA = California Consumer Privacy Act

CIPO = Company Information Privacy Orientation

CMB = Common Method Bias

CPA = Corporate Political Activity

CPPv = Corporate Political Privacy

CSA= Corporate Social Activism

CSR = Corporate Social Responsibility

CSPv = Corporate Social Privacy

CSV = Creating Shared Value

DCU = Dublin City University

DJT = Distributive Justice Theory

DPIA = Data Protection Impact Assessment

DV = Dependent Variable

IAPP = International Association of Privacy Professionals

IV = Independent Variable

FERPA = Family Educational Rights and Privacy Act

HIPAA = Health Insurance Portability and Accountability Act

HREIA = Human Rights Ethical Impact Assessment

FIPPs = Fair Information Privacy Practices

GRI = Global Reporting Initiative

GDPR = General Data Protection Regulation

ISO = International Standards Organisation

MIS = Management Information Systems

NME = Nonmarket Environment

NMPv = Nonmarket Privacy

PbD = Privacy By Design

PC = Privacy Concern

PII = Personally Identifiable Information

PJT = Procedural Justice Theory

PRE = Power Responsibility Equilibrium Theory

RALC = Restricted Access / Limited Control

RBV = Resource Based View

SCT = Social Contract Theory

SET = Social Exchange Theory

SPI = Sociopolitical Involvement

SPPv = Sociopolitical Privacy

SPSS = Statistical Package for the Social Sciences

PUBLICATIONS DEVELOPED FROM THE THESIS

Book Chapters

Lyons V. (2021). Justice vs Control in Cloud Computing: A Conceptual Framework for Positioning a Cloud Service Provider's Privacy Orientation. *IN*: Lynn T., Mooney J.G., van der Werff L., and Fox G. (eds) *Data Privacy and Trust in Cloud Computing.* Palgrave Studies in Digital Business & Enabling Technologies. Palgrave Macmillan, Cham.

Conference Proceedings

Lyons, V., van der Werff, L., and Lynn, T. (2020). Corporate Political Privacy: Quantitatively exploring the relationship between CPA and consumer trust, privacy concerns and purchase intentions. *EURAM, Trinity College Dublin*.

Lyons, V., van der Werff, L., and Lynn, T. (2020). Corporate Political Privacy: An Exploration of Privacy Lobbying, drawing on theories of Control and Justice, using an Experimental Vignette Methodology. *DCU Doctoral Colloquium,* Dublin

Lyons, V., van der Werff, L., and Lynn, T. (2019). The Politics of Privacy: An Exploration of Privacy Lobbying, drawing on theories of Control and Justice, using an Experimental Vignette Methodology. *Irish Academy of Management,* National College of Ireland, Dublin

Lyons, V., van der Werff, L. and Lynn, T. (2018). The Tao of Trust - Where Privacy and CSR Harmonise: A Qualitative Analysis Of Organisational Privacy Protection Disclosures In CSR Reports. *British Academy of Management,* Bristol.

Lyons, V. (2018). Doing Privacy Right Versus Doing Privacy Rights. *11th International Conference of Computers Privacy and Data Protection,* Brussels.

Lyons V., van der Werff, L. and Lynn, T. (2017). Compliance Versus Justice: Doing Privacy Right or Doing Privacy Rights. *Irish Academy Management*, Belfast.

Lyons V., van der Werff, L. and Lynn, T. (2016). Trust as Pacemaker: Regulating the Heart of Privacy. *First International Trust Conference (FINT),* Dublin.

Lyons V., van der Werff, L. and Lynn, T. (2016). Ethics as Pacemaker: Regulating the Heart of the Privacy-Trust Relationship. A proposed conceptual model. *International Computer and Information Systems (ICIS) Conference*, Dublin.

ABSTRACT

Valerie Lyons

'Doing Privacy Rights Versus Doing Privacy Right'

Examining the influence of nonmarket privacy activities on consumer trust, privacy concern and purchase/continuance intention.

Data breaches are rising in magnitude and cost, with technology and privacy threats advancing at a faster pace than privacy regulation. A more sustainable approach to privacy beyond regulation is required. Whilst privacy studies suggest that exceeding regulatory minimums reduces privacy incidents, there is a dearth of scholarship researching privacy activities beyond regulatory minimums. Organisations typically conduct activities beyond regulatory minimums in the nonmarket environment e.g., political and socially responsible activity. Thus, the nonmarket environment provides a starting point for insight into privacy activities beyond regulation.

This research utilises a three-stage sequential mixed-methods approach. Each stage is underpinned by theories of control and justice. In the first stage, an Online Delphi Survey is conducted to develop a taxonomy of control-based and justice-based nonmarket privacy activities. A theoretical framework of four primary approaches to privacy in the nonmarket environment is then developed. In the second stage, a number of CSR (CSR) reports (n=90) are reviewed using thematic analysis (leveraging the taxonomy previously developed). Control and justice totals are then calculated for the privacy activities reported in these publications, enabling their approach to nonmarket privacy to be positioned in one of four primary nonmarket privacy orientations. In the third stage, a theoretical framework is developed, based on the Power Responsibility Equilibrium (PRE) theory. Using this framework, a number of hypotheses are formulated regarding the relationships between nonmarket privacy activities and consumer trust, privacy concern, and purchase intention/continuance intention. These hypotheses are explored quantitatively using an experimental vignette methodology (n=396 for the first experiment, and n=503 for the second experiment). Control is found to be associated with increased privacy concern, and reduced consumer trust and purchase/continuance intention. Justice is found to be associated with reduced privacy concern, and increased consumer trust and purchase/continuance intention.

This research describes a typology of nonmarket privacy for the first time, and examines a previously unexplored phenomenon. This research extends PRE Theory to the context of nonmarket privacy activities. This research also extends CSR posture theory with the addition of an additional posture called the Warrior posture, and extends the three Generations of CSR with a Fourth Generation of CSR. The research findings provide insights which can assist organisations to address consumers' privacy concerns and enhance their corporate reputation and bottom line results.

1 CHAPTER ONE: INTRODUCTION

1.1 Dissertation Introduction

There is an abundance of literature exploring privacy activities in the consumer domain, however in the context of the nonmarket environment, privacy studies are rare. Using organisations' nonmarket environment publications regarding privacy, this dissertation examines the influence that levels of control and justice have on both the organisation's approach to nonmarket privacy (NMPv), and on the consumer's response to the organisation's NMPv activities. Due to the lack of scholarship in the phenomenon of privacy in the context of the nonmarket environment, the research is exploratory in nature, and aims to further our understanding of privacy in this context. To achieve this aim, a three stage sequential mixed methods research design was adopted.

This chapter begins by outlining the research aim and objectives. The justification for this research is then discussed. The research questions and overall research framework are then presented, followed by a summary of the key hypotheses. The chapter concludes with an overview of the dissertation structure.

1.2 Research Objectives

The overarching aim of this research is to develop a more comprehensive understanding of privacy in the nonmarket environment. This aim is represented by three key research objectives. The first objective is to develop a framework that explains NMPv approaches. Based on existing literature and the theoretical arguments presented by control and justice theory, a framework of four NMPv approaches is developed. This framework is referred to as the Nonmarket Privacy Orientation Matrix. Theories of Corporate Social Responsibility Postures (Castello and Lozano, 2009) and Corporate Social Responsibility Generations (Trapp, 2012) are leveraged to understand and explain these approaches. The second objective of this research is to construct a mechanism that can determine levels of control and justice signalled by their NMPv activities, and to use that mechanism to position an organisation's NMPv approach in one of the four orientations of the Nonmarket Privacy Orientations Matrix. The third objective is to explore the relationship between the levels of control and justice signalled by an organisation's NMPv activities, and outcomes for the consumer, namely privacy concern, consumer trust, and purchase intention/continuance intention. These objectives are represented in Figure 1.1.

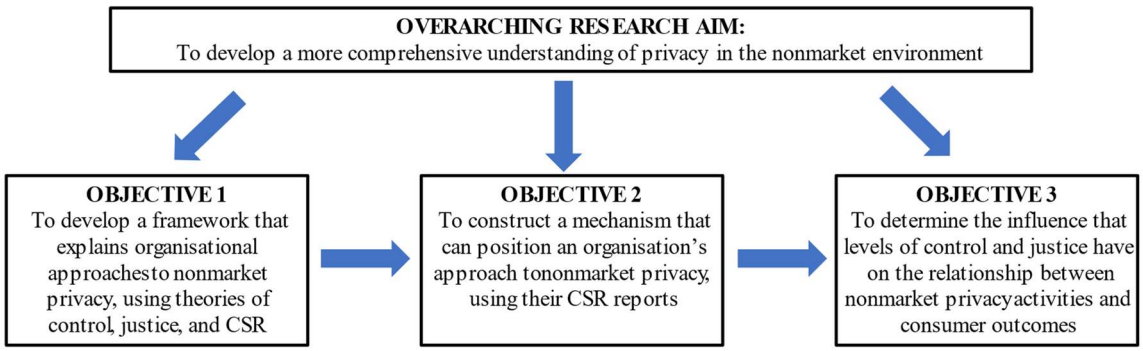


Figure 1.1 Research Aim and Objectives

1.3 Research Background

> *"Many nations have developed privacy protection laws and regulations to guard against unfettered government and private use of personal information. While these protections are important first steps in protecting privacy, existing laws and their conceptual foundations have become outdated because of changes in technology".*
>
> *(Laudon, 1996, p. 92)*

One might be forgiven for thinking that Professor Laudon's assertions were written recently – however they were written over twenty five years ago. Today, privacy protection laws and regulations continue to be the primary mechanism used by governments to guard against the misuse of personal data. Since Professor Laudon's assertions regarding the struggle of the regulatory lifecycle to keep pace with advances in technology (Laudon, 1996), there have been significant advances in technology - such as cloud computing, mobile, social media, and data analytics (Bauman and Lyon, 2013). Additionally, there have also been substantial increases in the number of digital transactions (Nagle et al., 2020) and in the amount of data collected (Yang et al., 2016), accelerating and amplifying the volume and velocity of data. With technology, data, and threats advancing at a faster pace than privacy regulation, data breaches continue to rise in frequency and magnitude (IBM and Ponemon Institute, 2020; Verizon, 2021). For instance, over the last 15 years, data breaches in the US have increased, from 57 data breaches in 2005 to 1001 data breaches in 2020 (Identity Theft Resource Center, 2020).

Organisations who experience a data breach can be subject to substantial financial cost, including the cost of remediation, legal liabilities, loss of brand image, customer trust, and ultimately market share and sales (Gwebu et al., 2018). These costs have risen by 12% over the past five years – with the average direct financial cost of a data breach in the US in 2020 reported to be between $3.6m and $7.13m (IBM and Ponemon Institute, 2020). Indirect costs associated with a data breach are more difficult to quantify, and include

reputational damage, loss of consumer confidence and consumer trust (IBM and Ponemon Institute, 2020; Laube and Böhme, 2016). Data breaches not only impact the consumer and the organisation, but are also a real concern for managers, investors and regulators (IBM and Ponemon Institute, 2020). In addition to the continued rise in data breaches, the regulatory response to privacy also presents a number of challenges. First, mandatory breach disclosure – a core element of privacy regulation – is predicated on detecting or prosecuting a violation, only after it has occurred and the damage is done (Solove, 2006). Second, regulations are often reactive and lagging technology by the time they are enacted (Culnan and Williams, 2009). For instance, the General Data Protection Regulation was in discussion for four years, before being approved by the EU parliament in 2016, coming into force then only two years later[1].

Thus, whilst challenges associated with privacy continue to grow, the ineffectiveness of the regulatory responses to these challenges continues to grow also - and a more sustainable approach to privacy, beyond regulatory minimums, needs to be considered. Addressing privacy beyond regulatory minimums is important for privacy effectiveness, as commentators suggest that organisations who protect information in a way that exceeds regulatory minimums experience less privacy incidents (Accenture and Ponemon Institute, 2015). If organisations did more than simply adhere to privacy legislation, they would be more effective at protecting consumer data and experience less data breaches (Cavoukian et al., 2014). Thus, organisations could avoid the potential negative effects associated with a data breach, such as reduced consumer spending (Janakiraman et al., 2018), or decreased consumer trust (Martin et al., 2017). Bart Willemsen, Vice President at Gartner, highlights how building privacy programs that proactively address privacy, rather than simply respond to regulation, increase consumer trust (Gartner, 2020). In other words, doing

[1] International Network of Privacy Law Professionals: https://inplp.cust om/latest-news/article/a-brief-history-of-data-protection-how-did-it-all-start/.

privacy right rather than simply doing privacy rights may present a more effective approach to privacy, one associated with reduced data breaches and more positive corporate and consumer outcomes.

However, there is a dearth of scholarship researching privacy activities exceeding regulatory minimums, or the influence these activities may have on outcomes for the organisation or their key stakeholders. Filling this gap, this research builds on explorations of privacy in the Information Systems (IS) literature, and integrates them with studies of the nonmarket environment. The nonmarket environment context was chosen, as it is where an organisation's discretionary activities beyond regulatory requirements are typically conducted and reported. The importance of, and need for, this research is discussed in the remainder of this section across the following key areas:

(i) the importance of the nonmarket environment,

(ii) understanding the potential effects of privacy in the nonmarket environment,

(iii) understanding how privacy in the nonmarket environment influences consumers, and

(iv) introducing a typology of privacy in the nonmarket environment.

1.3.1 The Importance of the Nonmarket Environment

The nonmarket environment, together with the market environment, represent the two main streams of interactions that an organisation has with its stakeholders (Baron, 1995). In the market environment, organisations undertake activities that directly shape profitability - such as lowering costs, increasing prices or revenue, marketing and advertising and enhancing response times. In the nonmarket environment, organisations undertake activities that indirectly shape profitability, such as advising public policy, building coalitions, influencing regulators, influencing governments, and managing media.

The nonmarket environment is important for organisations, as an organisation's activities in the nonmarket environment can drive competitive advantage, improve risk management, foster innovation, enhance financial performance, build customer loyalty and attract/engage employees (Fink and Whelan, 2016). The nonmarket environment is also of interest to investors, as investors increasingly use organisations' nonfinancial disclosures to inform their investment decisions (Ernst and Young, 2018). Reflecting this interest, responsible investment indexes such as the FTSE4Good have emerged to help investors identify companies that meet globally recognised corporate responsibility standards (Charlo et al., 2015). The nonmarket environment is also of growing interest to researchers. For example, in 2021 the Journal of Management Studies launched a call for papers for a special issue on corporate social and political strategic objectives. The call highlighted how compared to the voluminous research on conventional business strategy, academic inquiries into nonmarket environment strategies have been slow to develop. The call also highlighted the lack of an integrative understanding of how organisations develop relationships with their social and political stakeholders in nonmarket environments (Lawton et al., 2014; Mellahi et al., 2016; Scherer et al., 2016).

How an organisation interacts with its nonmarket environment is referred to as its nonmarket strategy (Lux et al., 2011; Wrona and Sinzig, 2018). The prominent nonmarket strategies are Corporate Social Responsibility (CSR) and Corporate Political Activity (CPA) (Doh et al., 2012; Funk and Hirschman, 2017; Lawton and Rajwani, 2015). More recently, Sociopolitical Involvement (SPI) has been proposed as an additional nonmarket strategy (Nalick et al., 2016). Nonmarket strategies can enable entry into new markets, reduce regulation, disable rivals, limit price increases, and raise the costs for competitors (Liedong et al., 2014). Studies have shown that CSR can reduce an organisation's exposure to risk (Godfrey, 2005; Lou and Bhattacharya, 2009) and improve firm reputation, consumer trust, and long-term loyalty (Chernev and Blair, 2015; Homburg et al., 2013).

Similarly, CPA can increase an organisation's performance outcomes as a result of reducing uncertainty in the nonmarket environment (Hillman and Hitt, 1999).

1.3.2 Privacy in the Context of the Nonmarket Environment

The extant privacy and nonmarket environment literature has largely neglected privacy-specific nonmarket strategies. For instance, a recent systematic review of the nonmarket environment literature by Wrona and Zinzig (2018) did not reference any studies that relate to privacy within the context of the nonmarket environment. In 2011, MISQ published two literature reviews of privacy in a special issue (i.e., Belanger and Crossler, 2011; Smith et al., 2011). Neither of these reviews referenced privacy in the context of the nonmarket environment (i.e., privacy as a CSR, privacy as a CPA, or privacy as an SPI). A search of the privacy, management, IS, and business ethics literature - for privacy in the context of the nonmarket environment - found that only three notable papers between 2005 and 2015 referenced privacy as a CSR (i.e., Allen and Peloza, 2015; Ashworth and Free 2006; Pollach 2011). This interest in privacy as a CSR appears to be gaining momentum, as more recent studies referencing privacy as a CSR are increasingly emerging (e.g., Bandara et al., 2020; Lobschat et al., 2021; Martin, 2020; Schultz and Seele, 2019; Shilton and Greene, 2019). Privacy as a CSR is also included in several standards for CSR reporting. For example, section 6.3.4 of the International Standards Organisation for Social Responsibility 'ISO 26000', refers to privacy as a Human Right, and section 6.7.7 refers to consumer privacy (International Standards Organisation, 2021). Section 418 of the Global Reporting Initiative (GRI) also addresses consumer privacy (Global Reporting Initiative, 2021).

Whilst some scholars have noted that the evolution of digital technologies raises matters of political concern, they do not attend directly to CPA or SPI (Murray and Flyverbom, 2021). Thus, there still remains a paucity of research investigating privacy as a CPA or

privacy as an SPI. This would indicate that whilst privacy in the context of the nonmarket environment is a subject of growing interest to scholars, the conversation has not yet extended beyond privacy as a CSR. This under-examination of privacy in the context of the nonmarket environment is problematic for three reasons. First, privacy is an issue of fundamental importance to society (Margulis, 2003) and is considered a first-level societal concern (Westin, 2003). Second, privacy activities can enhance or damage an organisation's bottom line and reputation (Centrify and Ponemon Institute, 2017), as too can nonmarket environment activities (Lawton et al., 2012; Wrona and Sinzig, 2018). Third, the number of organisations undertaking privacy as a CSR and CPA is on the rise. For instance, Forrester (2018) found that of the Fortune 100 organisations in 2016 and 2017, twenty-one framed privacy as a nonmarket activity in their CSR reports, growing in 2018 to twenty-eight. Big Tech organisations such as Google, Facebook, Apple, Microsoft and Amazon are increasingly investing millions of dollars every year in privacy specific lobbying (VpnMentor, 2019).

Whilst there is evidence that privacy activities are conducted in the nonmarket environment, there is little guidance on the influence that such activities have on stakeholders. This is an important gap to fill, as organisations need to understand the impact their activities have on the extended stakeholder community, including the broader economy, the environment and the society in which they operate (Savitz, 2013). Organisations may, for instance, undertake privacy activities that negatively impact both their market and nonmarket environments, or they may miss opportunities to engage with privacy activities that positively impact both these environments. If through nonmarket strategies and their associated activities, positive firm performance outcomes result (Chernev and Blair, 2015; Homburg et al., 2013) then privacy-specific NMPv activities may impact those same positive firm performance outcomes. In this dissertation, the protection of privacy emerges as a major means by which organisations can influence and

interact with their nonmarket environment and thus enhance/damage their relationship with their consumer and therefore their bottom line.

An organisation's privacy activities have been found to influence an individual's concern for privacy (Smith et al., 2011), trust (Lauer and Deng, 2007; Liu et al., 2005; Wu et al., 2012) and intentions (Hui et al., 2007; Meinert et al., 2006; Peterson et al., 2007). The importance of these constructs is well established in the privacy literature. However, with the exception of Bandara et al. (2020), who explore the influence of an organisation's ethical data practices (which they call 'Corporate Privacy Responsibility') on consumer trust, the literature has yet to explore the influence of an organisation's privacy activities on these constructs in the nonmarket environment. This is important, as organisational activities in the nonmarket environment have been found to influence both consumer trust (Castaldo et al., 2009; Choi and La, 2013; Martínez and del Bosque, 2013) and their purchase intention (Creyer, 1997). A comprehensive understanding of how an organisation's NMPv activities influences these constructs may help organisations to develop more effective privacy practices and develop a broader privacy management strategy. This research addresses this, by exploring how privacy activities associated with predominant nonmarket environment strategies influence a consumer's privacy concern, their trust in the organisation, and their purchase intention/continuance intention.

This research finds that NMPv activities reflecting values of justice and responsibility lead to increased consumer trust and purchase intention/continuance intention, and reduced privacy concern. In contrast, NMPv activities reflecting values of control and power are found to lead to increased privacy concern and decreased consumer trust and purchase intention/continuance intention. For two reasons, this is an important insight for organisations into the potential influence that NMPv activities can have on the consumer. First, increases in consumer trust in an organisation can lead to increases in consumer engagement, purchasing, brand loyalty, investor interest, etc. (Edelman, 2020). Second,

increases in privacy concern can lead to stakeholders taking negative defensive measures such as fabricating, withholding, or protecting (Lwin et al., 2007). This research also highlights the potential for justice-based CPA, called 'deliberative lobbying' (Lock and Seele, 2017; Seele and Lock, 2015), to enhance the consumer-trust relationship, and for control-based CPA, called 'instrumental lobbying' (Lock and Seele, 2017), to damage it. This is a particularly important insight for large technology organisations, as privacy was the most frequently used word in Big Tech lobbying submissions between 2005 and 2018 (VpnMentor, 2019).

1.3.3 The Need for a Typology of Nonmarket Privacy

The lack of typology for NMPv activities and NMPv approaches, serves to highlight a gap in our knowledge. In describing the phenomenon of privacy in the nonmarket environment for the first time, a common language for future dialogue and research is established. Figure 1.2 presents a conceptual typology for privacy in the nonmarket environment, as presented in this dissertation.

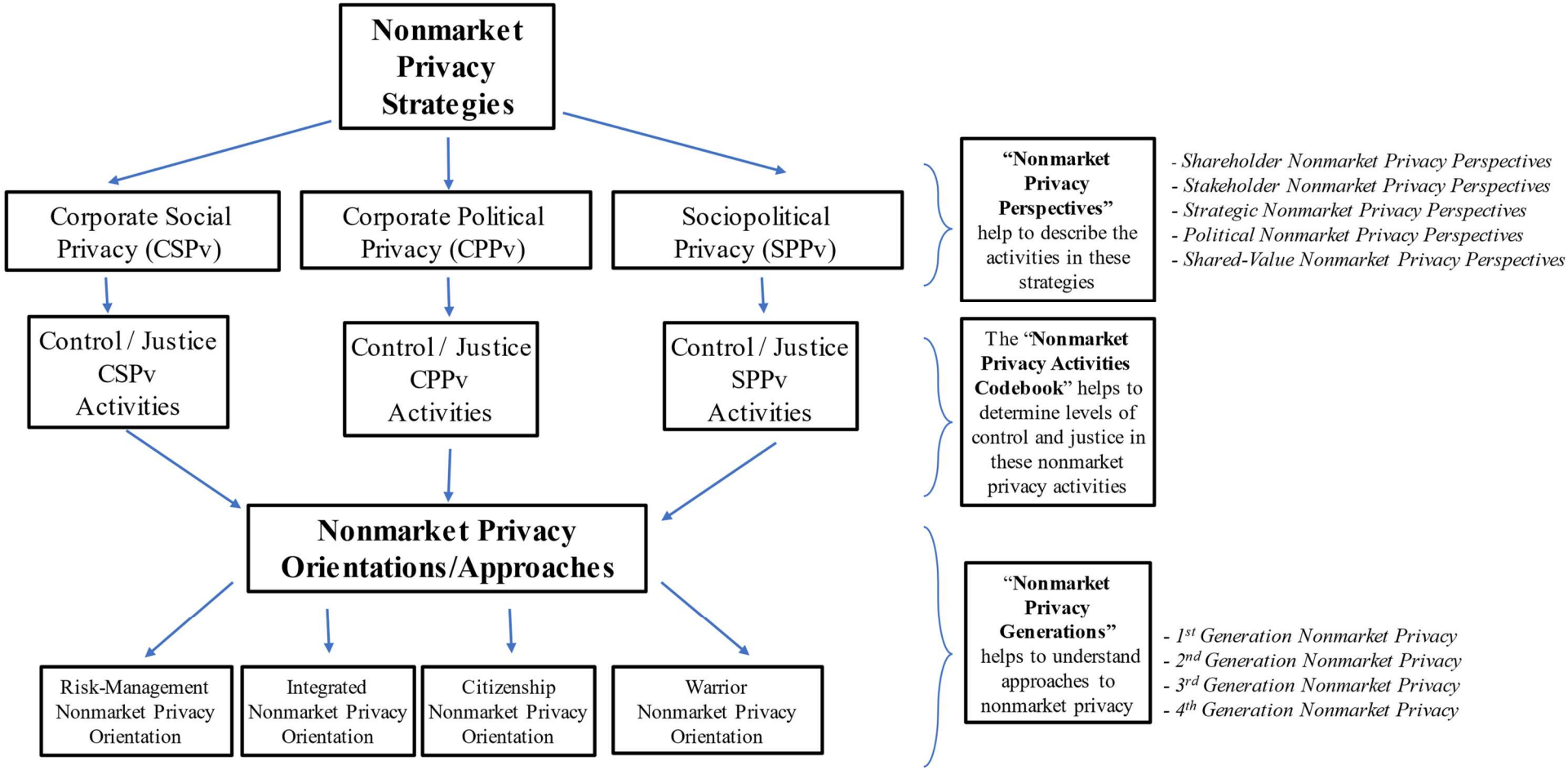


Figure 1.2 Typology of Nonmarket Privacy

By integrating concepts of privacy over four decades with the key nonmarket strategies of CSR, CPA and SPI, a set of NMPv strategies are presented in this research, namely Corporate Social Privacy, Corporate Political Privacy and Sociopolitical Privacy. The NMPv activities associated with these NMPv strategies are then used to form the Nonmarket Privacy Activities Codebook. By integrating current approaches to privacy with current approaches to nonmarket environment strategies, a set of four primary NMPv approaches are also presented. These approaches form the Nonmarket Privacy Orientations Matrix. Table 1.1 presents an explanation of the NMPv terms established throughout this research.

Table 1.1 Definitions/Descriptions of the Nonmarket Privacy Terms Proposed in this Research

Term	Dimensions	Definition/Description
Nonmarket Privacy Activity (NMPv)	Control based NMPv Justice based NMPv	Any privacy activity that an organisation undertakes as part of their nonmarket program or agenda.
Nonmarket Privacy Strategy	Corporate Social Privacy (CSPv)	An evolving umbrella term for a variety of concepts and practices, which recognise that organisations have a societal responsibility towards privacy, beyond legislation and liability.
	Corporate Political Privacy (CPPv)	Corporate attempts to shape government policy and regulation regarding privacy.
	Sociopolitical Privacy (SPPv)	An organisation's public demonstration (statements and/or actions) of support for or against privacy as a sociopolitical issue, with no direct performance motivation.
Nonmarket Privacy Orientations	Determined by the level of control and justice established by their NMPv activities, as reported in their nonmarket publications	An organisation's approach to, and understanding of, its legal, social and political responsibilities towards protecting privacy, the NMPv programs it develops to implement privacy protection, and how it frames and communicates its privacy activities.
	Risk Management Orientation	Organisations in this orientation set privacy compliance as the goal, where governance is assigned to functional management, and neither vision nor mission, are related to CSR activities.
	Integrated NMPv Orientation	Organisations in this orientation offer robust compliance to regulation as a baseline, whilst recognising and minimising the limitations of bare compliance.
	Citizenship NMPv Orientation	Organisations in this orientation are focused on building and maintaining sustainable relationships by reaching out to stakeholders and associating their Corporate Social Privacy activities with other strong values such as trust and integrity.
	Warrior NMPv Orientation	Organisations in this orientation take a revolutionist approach to nonmarket activities. The Warrior organisation will participate in protests, breach laws and even alienate certain stakeholders in order to address privacy as a social issue.

Term	Dimensions	Definition/Description
Nonmarket Privacy Perspectives: *CSPv Perspectives*	Stakeholder CSPv Perspectives	The Stakeholder CSPv perspective assumes that organisations consider the privacy concerns of multiple constituencies including employees, suppliers, consumers, local communities etc.
	Strategic CSPv Perspectives	In the Strategic CSPv perspective, privacy is driven by organisational concerns about generating value, from market-based solutions that address privacy in a socially responsible way.
	Political CSPv Perspectives	In the Political CSPv perspective, activities beyond traditional Corporate Social Privacy are conducted, placing firms in quasi-governmental roles in which major decisions regarding privacy, as a matter of public welfare and social provision, are made.
	Creating Shared Value CSPv Perspectives	In the Creating Shared Value perspective, responsibilities towards privacy are integrated to, and from, all stakeholders. The central premise behind the shared value perspective is that the competitiveness of an organisation, and wellbeing of the communities around it with regard to privacy, are mutually dependent.
Nonmarket Privacy Perspectives: *CPPv Perspectives*	Instrumental CPPv Perspectives	Short-term; where an organisation's privacy-specific lobbying activity is judged by the private returns it brings to the organisation.
	Transactional CPPv Perspectives	Short-term; organisations await the development of an important privacy issue before formulating a strategy (i.e., Corporate Political Privacy) in response.
	Relational CPPv Perspectives	Long-term; organisations pursue Corporate Political Privacy activities over the long term, rather than on an issue-by-issue basis. Organisations build relationships so that when privacy-related policy issues that affect their operations arise, the contacts and resources needed to influence this policy are already in place.
	Responsible CPPv/Deliberative CPPv Perspectives	Long-term; when an organisation tries to shape the rules for privacy in a way that balances the common good together with the corporate good or in a way that aims to resolve a public issue.
Nonmarket Privacy Perspectives: *SPPv Perspectives*	Corporate Sociopolitical Privacy Perspectives	An organisation's public demonstration of support for, or in opposition to, one side of a Sociopolitical Privacy issue, issuing statements and/or undertaking actions.
	CEO Sociopolitical Privacy Perspectives	Corporate leaders speaking out on Sociopolitical Privacy issues not directly related to their company's core business.
	Shareholder Sociopolitical Privacy Perspectives	Actions taken by shareholders with the explicit intention of influencing corporations' privacy policies and practices, rather than the latent intention of ownership stakes or trading behaviour.

1.3.4 Summary: The Importance of this Research

The importance of this research is justified on four grounds. First, as noted in the previous sections, there is a dearth of scholarship exploring privacy in the context of the nonmarket environment. Addressing this dearth is important, as an organisation's activities in the nonmarket environment can influence outcomes for both the organisation and for the consumer. Responding to this, this research introduces a NMPv taxonomy and explores associated NMPv strategies, activities, orientations and outcomes. This research also responds to several calls in the literature, as outlined in Table 1.2.

Table 1.2 How the Research Responds to Calls in the Literature

Calls In The Literature	How This Research Responds
Venkatesh et al. (2013), for instance, call for more mixed-methods studies in the IS literature.	This research uses a mixed methods approach to privacy research. The integrated quantitative and qualitative findings of this research enable the presentation of practical recommendations, which can be employed by organisations to address the consumer privacy concerns and trust issues that can result from an organisation's NMPv activities. These findings also lead to several potential avenues for further research in this area.
Smith et al. (2011) call for more theory-based privacy studies.	This research applies theories of control and justice to construct a framework of four primary NMPv approaches.
Frynas et al. (2017) call for more power-based approaches to nonmarket research.	This research uses power responsibility equilibrium (PRE) theory to explain the influence of NMPv activities on the consumer.
In the Journal of Management Studies, Luo et al. (2021) published a call for papers seeking further research in CPA, CSR and SPI.	This research determines the NMPv activities associated with the three nonmarket strategies (i.e., CSR, CPA and SPI) and determines the levels of control and justice signalled by those NMPv activities.

Second, whilst Lwin et al. (2007) and Greenaway et al. (2015) both present a comprehensive understanding of the challenge between privacy, regulators and consumers, this dissertation extends and builds on their work, to provide a more nuanced understanding of organisations' approaches to privacy and their influence on consumer responses. This research thus expands existing privacy theory in three ways by:

- Integrating CIPO (Greenaway et al., 2015) and the PRE Model of Privacy (Lwin et al., 2007) to extend our understanding of how power and responsibility are enacted in organisation-consumer relationships.
- Expanding the outcomes associated with the PRE Model of Privacy.
- Extending our understanding of the organisational factors involved in a consumer's privacy-related decision making.

Third, by applying existing theories of privacy and existing theories of CSR to a previously overlooked context, i.e., privacy in context of the nonmarket environment, this research deepens our understanding of the phenomenon. By combining theories of privacy with theories of the nonmarket environment, the researcher asserts that privacy can engender benefits associated with the nonmarket environment, such as increased consumer trust and brand loyalty (Glaveli, 2020), and extends these benefits to include reduced privacy concerns.

Fourth, by combining existing theories of privacy and existing theories of the nonmarket environment, new outputs are devised that help to understand privacy in the context of the nonmarket environment more comprehensively. For example, by combining perspectives of privacy and perspectives of the nonmarket environment over four decades, a set of perspectives of NMPv emerge, that explain a progression of privacy thinking, previously not described. By combining nonmarket strategies (CSR, CPA, SPI) with privacy, a set of NMPv strategies are presented, i.e., Corporate Social Privacy, Corporate Political Privacy, Sociopolitical Privacy, together with a set of associated nonmarket privacy activities. By combining current approaches to privacy i.e., CIPO from Greenaway et al. (2015) with approaches to CSR i.e., CSR Postures from Castello and Lozano (2009), a set of four approaches to NMPv are presented.

1.4 Research Questions and Framework

The research objectives, outlined in Section 1.2, are considered in the following three research questions:

RQ1: What are the key privacy activities in the nonmarket environment, and what level of control or justice do these activities signal?
RQ2: Can an organisation's approach to nonmarket privacy be determined from their published nonmarket privacy activities?
RQ3. What influence do levels of control and justice, signalled by nonmarket privacy activities, have on privacy concern, consumer trust and purchase intention/continuance intention?

The overall research framework, outlined in Figure 1.3, explores these questions by investigating organisational approaches to NMPv and examining the influence that control and justice has on those approaches and on outcomes for the consumer, i.e., privacy concern, consumer trust and purchase intention/continuance intention. The framework is underpinned by PRE Theory (Davis et al., 1980). In PRE theory, the power holders are expected to exhibit equality with less powerful partners. The inability to do so will result in forces curtailing power, demanding more responsible actions, or both, to maintain an equilibrium. In the PRE Model of Privacy (Lwin et al., 2007), consumers who perceive that organisations are acting responsibly in terms of their privacy practices, are expected to have more trust in the organisation and express less concern for privacy (Lwin et al., 2007). Building on the PRE Model of Privacy (Lwin et al., 2007), the research framework applied in this dissertation suggests that levels of control (representing power) and justice (representing responsibility) signalled by an organisation's NMPv activities, influence both organisational approaches to privacy, and consumer responses. The research framework posits that both an organisations approach to nonmarket privacy, and a consumer's response to NMPv activities, is influenced by the levels of control and justice that NMPv

activities signal. Control-based NMPv activities increase the consumer's privacy concern, reduce their trust in the organisation, and reduce their purchase intention/continuance intention. In contrast, justice-based NMPv activities decrease the consumer's privacy concern, increase their trust in the organisation, and increase their purchase intention/continuance intention.

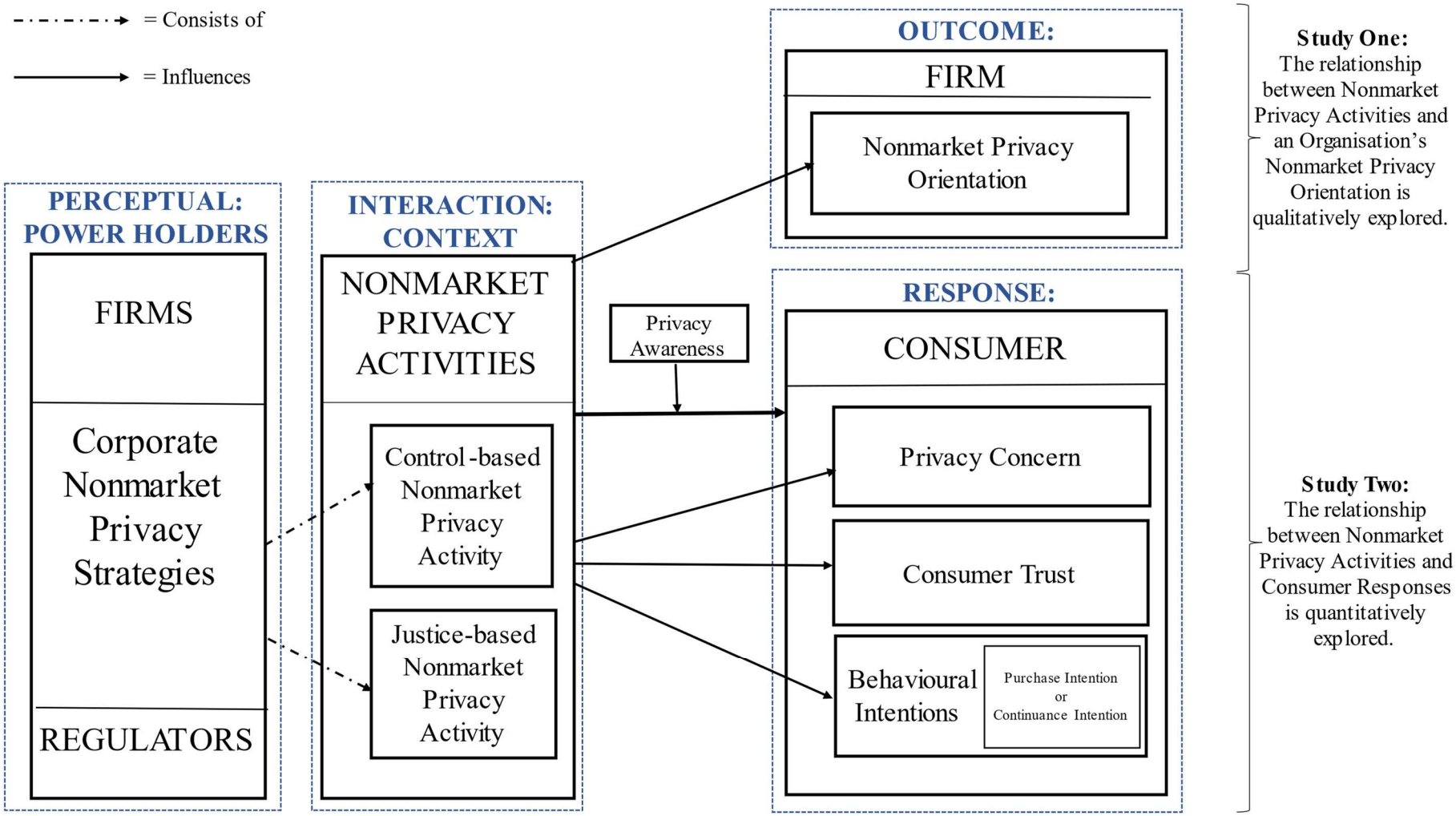


Figure 1.3 Overall Research Framework

1.5 Key Hypotheses

The following hypotheses in Table 1.3 are developed based on the literature review.

Table 1.3 Key Hypotheses.

H1:	An organisation's reported NMPv activities signalling high levels of control are positively related to privacy concern.
H2:	An organisation's reported NMPv activities signalling high levels of justice are negatively related to privacy concern.
H3:	An organisation's reported NMPv activities signalling high levels of control are negatively related to consumer trust.
H4:	An organisation's reported NMPv activities signalling high levels of justice are positively related to consumer trust.
H5:	An organisation's reported NMPv activities signalling high levels of control are negatively related to a) purchase intention or b)continuance intention
H6:	An organisation's reported NMPv activities signalling high levels of justice are positively related to a) purchase intention or b)continuance intention.
H7:	Privacy awareness positively moderates the relationship between NMPv activities and privacy concern; such that the relationship is stronger when privacy awareness is high than when it is low.
H8:	Privacy awareness negatively moderates the relationship between NMPv activities and consumer trust; such that the relationship is stronger when privacy awareness is low than when it is high.
H9:	Privacy awareness negatively moderates the relationship between NMPv activities and continuance intention; such that the relationship is stronger when privacy awareness is low than when it is high.

1.6 Research Methodology

A three-stage, sequential, mixed methods research design was adopted, as outlined in Figure 1.4.

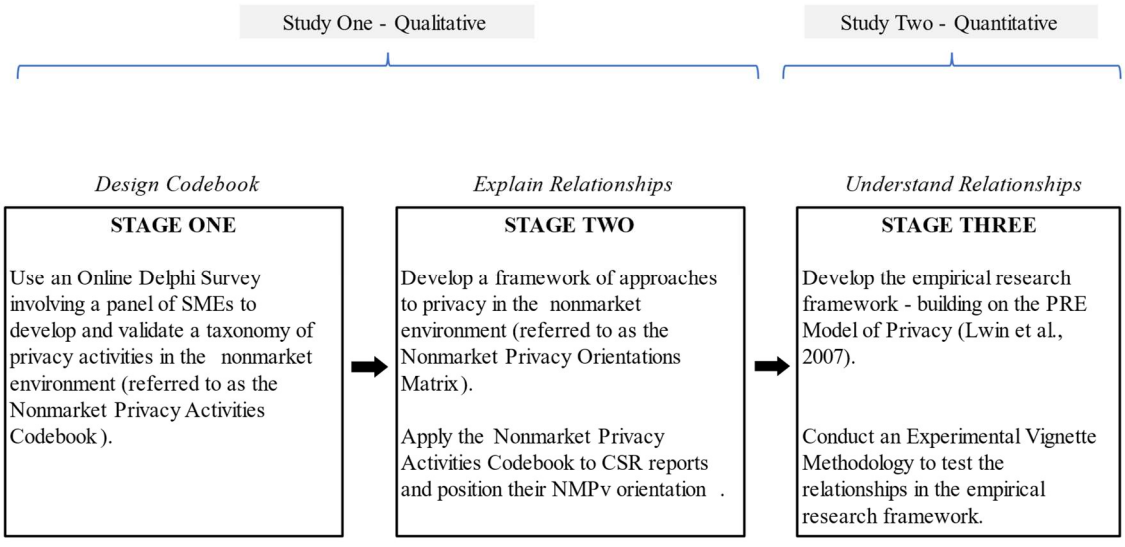


Figure 1.4 Overall Research Design

In the first stage, leveraging a panel of experts in an Online Delphi Survey, a taxonomy of control-based and justice-based NMPv activities is developed. This is referred to as the Nonmarket Privacy Activities Codebook. The codebook is intended to be used to determine an organisation's approach to NMPv. Progressing to the second stage, the Nonmarket Privacy Orientations Matrix is developed, which is a theoretical 'map' of four primary approaches to NMPv, characterised by levels of control and justice signalled by NMPv activities.

To demonstrate operability of the Nonmarket Privacy Activities Codebook, and to determine an organisation's NMPv orientation, the codebook is qualitatively applied to the CSR reports *(n=90)* of the organisations in the Fortune 100 index. This stage leverages the matrix approach to thematic analysis (Groenland, 2018) and is conducted using NVivo. The third stage uses an experimental vignette methodology (EVM) (Aguinis and Bradley, 2014) to quantitatively determine the influence that levels of control and justice, signalled by different NMPv activities, have on consumer responses. The sample comprises North American Amazon Mechanical Turk (AMT) workers. The experiment leverages ANOVA/ANCOVA as the key statistical tests and is conducted using IBM's SPSS tool. The findings provide strong empirical support for the influence of control and justice on the relationship between an organisation's NMPv activities and consumer responses. The quantitative and qualitative findings are integrated to deepen our understanding of privacy in the context of the nonmarket environment.

1.7 Dissertation Outline

The dissertation consists of seven chapters. The structure of this dissertation, in terms of the objective of each chapter, is outlined in Figure 1.5.

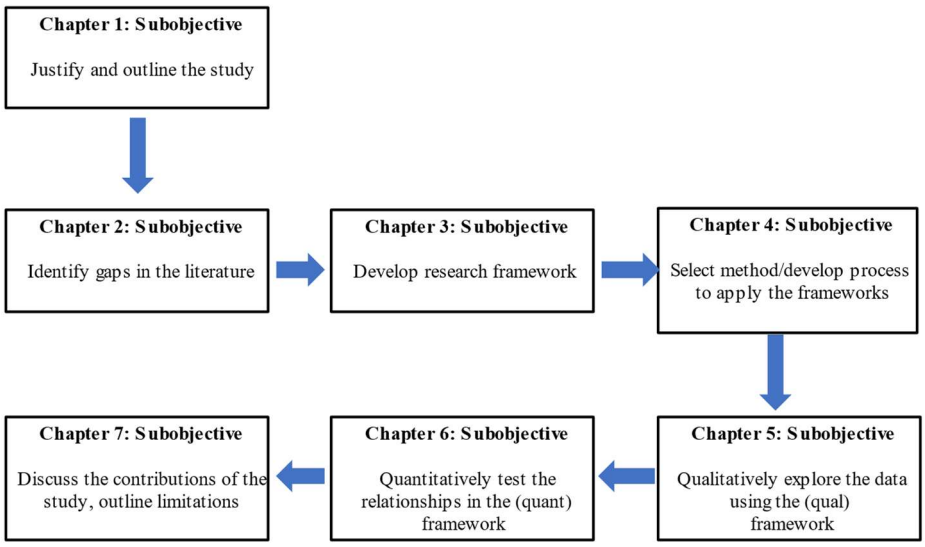


Figure 1.5 Dissertation Structure Overview

Chapter One justifies the need for the research and details the research objectives, research questions, and key hypotheses. In Chapter Two, the existing literature is critically examined stemming primarily from fields of privacy, IS, business ethics, and the nonmarket environment. The aim of the literature review is to identify gaps in our understanding of privacy in the context of the nonmarket environment, as well as theories and constructs pertinent to addressing these gaps. The literature review examines past works and theoretical arguments pertaining to privacy and nonmarket environment strategies, and in particular to how theories of control and justice are applied.

Chapter Three builds upon the literature review to present the proposed research model(s), and the hypotheses to be tested in the research. Characterised by theories of control and justice, a framework is developed to explain four primary organisational approaches to NMPv, referred to as the Nonmarket Privacy Orientation Matrix. This framework forms

the primary research framework for Study One. Theories of control and justice are then interpreted as power and responsibility to form the quantitative research framework for Study Two. The research framework for Study Two is based on Power Responsibility Equilibrium (PRE) Theory (Davis et al., 1980) and builds on the PRE Model of Privacy (Lwin et al., 2007; Krishen et al., 2017), thus extending the application of PRE Theory to explore privacy in the context of the nonmarket environment for the first time.

Chapter Four discusses the philosophical assumptions underpinning this research and provides a detailed overview of the three-stage, sequential, mixed methods research design and the sampling procedures followed in each stage. Chapter Five discusses the qualitative data analysis procedures for Study One. First presented is the Online Delphi Survey used to develop a taxonomy of control-based and justice-based NMPv activities. The application of this taxonomy, using a thematic analysis of a sample of CSR reports, is then discussed. Chapter Six presents the quantitative analysis to support the findings. This chapter concludes with a discussion of the integrated findings of both the qualitative and quantitative studies. Chapter Seven discusses the contributions of the research and presents the revised research model along with several theoretical assumptions. Chapter Seven also discusses the implications for practice and policymakers, and concludes with the limitations inherent in the research and directions for future research.

2 CHAPTER TWO: LITERATURE REVIEW

2.1 Chapter Introduction

This chapter aims to establish the current level of knowledge of privacy in the nonmarket environment and identify gaps in our understanding of privacy in this context. The chapter also provides an overview of relevant theories and constructs that are leveraged to address the research questions. The chapter begins by providing some background as to why the nonmarket environment was chosen for the context of this research, and then briefly recaps the research questions. This is followed by an overview of how control and justice theories are used in the privacy and nonmarket environment literature. As an understanding of the nonmarket environment is foundational to the context of this thesis, the nonmarket environment is discussed, outlining key definitions and strategies. Next, a discussion of privacy in the nonmarket environment is presented, starting with a discussion of the evolution of privacy and key definitions. As this dissertation focuses on privacy concern, consumer trust, and purchase intention/continuance intention, the relationship between these constructs, in both the privacy and the nonmarket environment literature, is presented. The chapter concludes with a brief summary of the gaps in the literature.

The literature review is presented visually in Figure 2.1.

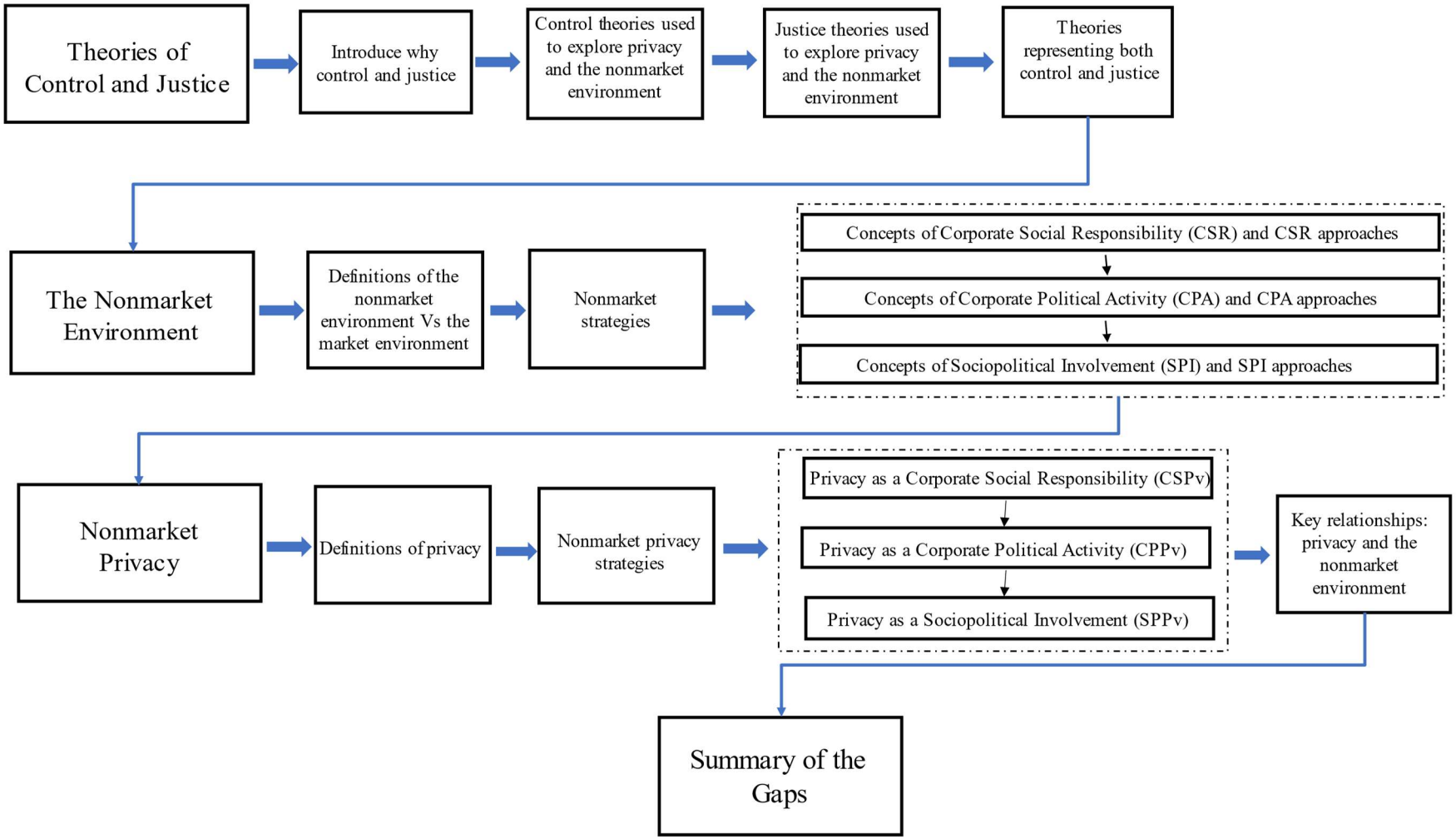


Figure 2.1 Literature Review Overview

2.2 Background and Research Questions

Traditional organisational approaches to privacy have focused on conducting privacy activities associated with strict regulatory compliance. Such approaches risk overlooking the potential benefits associated with conducting privacy activities beyond regulatory minimums, such as increased trust (Cavoukian, 2016), decreased privacy concern (Xu, 2009) and reduced privacy incidents (Accenture and Ponemon Institute, 2015). Beyond the privacy and nonmarket environment literature, several studies in the law literature highlight the need for privacy regulation to address privacy as a social, political and/or ethical concern (Butterworth, 2018; Mantelero, 2018; Raab, 2020). Mantelero (2018), for instance, argues the need for collective interests beyond the individual's rights be considered in order to address privacy, and suggests integrating human rights, social concerns and data protection rights.

An organisation's activities related to human rights and social, legal and political practices, are conducted in their nonmarket environment and reported in their nonmarket publications, such as their CSR reports. To gain insight into privacy activities beyond regulatory minimums, the business ethics literature presents a starting point, where Pollach (2011) explores privacy activities beyond regulation using an organisation's reported privacy activities in their CSR reports. Thus, this chapter extends beyond the privacy literature to include the nonmarket environment literature in order to explore organisational privacy activities beyond regulation and their influence on consumer responses.

Prior to discussing the extant privacy and nonmarket environment literature, the research questions outlined in Chapter One are presented. Exploratory in nature, this research aims to develop a comprehensive understanding of privacy in the nonmarket environment, and addresses this broad aim under these three research questions:

RQ1: What are the key privacy activities in the nonmarket environment, and what level of control or justice do these activities signal?
RQ2: Can an organisation's approach to nonmarket privacy be determined from their published nonmarket privacy activities?
RQ3. What influence do levels of control and justice, signalled by nonmarket privacy activities, have on privacy concern, consumer trust and purchase intention/continuance intention?

In order to determine an approach to respond to these questions, the nonmarket environment and privacy literature was reviewed, to explore the application of control and justice theories in the literature and gaps in our current understanding.

2.3 Theories of Control and Justice

To date, a number of theories have been leveraged to examine privacy across several disciplines. Several studies apply more than one theory, as some theories explain the factors predicting concern for privacy, while others seek to understand the outcomes of privacy (Li, 2012). In the nonmarket environment literature, Mellahi et al. (2016) highlight that control-based theories such as agency theory and institutional theory, are associated more often with CPA, whilst justice-based ethical theories such as stakeholder and stewardship theory, are most often associated with Corporate Social Responsibility. In the privacy literature, Greenaway et al. (2015, p. 580) present a theoretical framework of privacy approaches called Company Information Privacy Orientation (CIPO), which explores how different organisations reconcile and balance privacy challenges. CIPO is defined by Greenaway et al. (2015) as an organisation's approach to protecting and using customer information, and they interchangeably refer to this approach as a privacy 'orientation' or 'posture'. An organisation's CIPO is determined by the level of control and justice demonstrated in their legal, financial, and ethical behaviours. By differentiating the

extent to which control and justice influence an organisation's privacy activities, CIPO reflects the extent to which organisations' privacy policies affect their customers' abilities to exercise control and justice mechanisms over the collection and use of their personal information (Greenaway et al., 2015).

The combination of control and justice characterising the CIPO framework forms the starting point for this research. Greenaway et al. (2015) call for the construction of a mechanism that can position an organisation's privacy posture, based on a measurement of the amount of control and justice signalled by an organisation's privacy activities. Finding that no such mechanism exists and recognising its potential importance, this research seeks to construct such a mechanism, in the context of an organisation's NMPv activities. In the remainder of this section, the application of control and justice in the privacy and nonmarket environment literature is outlined. These theories are summarised in Figure 2.2.

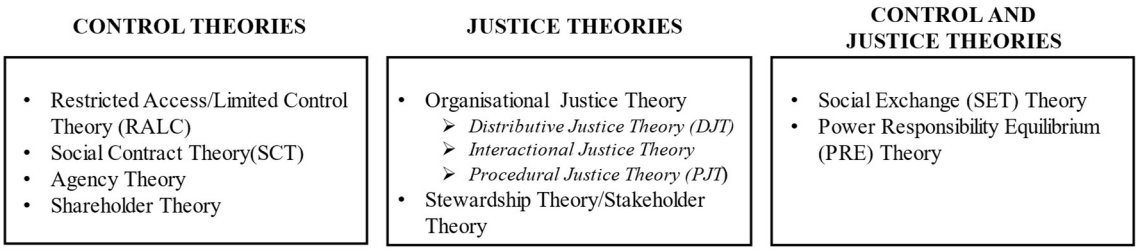


Figure 2.2 Control and Justice Theories

First discussed are theories of control, followed by theories of justice, and lastly theories of control and justice. These theories will help address the first research question: *RQ1: What are the key privacy activities in the nonmarket environment, and what level of control or justice do these activities signal?*

2.3.1 Theories of Control

While there is no single concept of information privacy that crosses all disciplines, control over personal information is a common theme (Belanger and Crossler, 2011). There is ambiguity in the literature, however, as to what exactly the notion of control means. For instance, some scholars argue that privacy is determined by the ability 'to control' personal information (Tavani, 2000), where others view privacy as 'the controls' in place over uses of personal data for purposes other than originally intended (Belanger et al., 2002).

Control is frequently explored in the literature at the individual level and associated with privacy concerns (Fox et al., 2021; Malhotra et al., 2004; Pavlou and Fygenson, 2006; Phelps et al., 2000; Xu, 2007), trust and self-disclosure behaviour (Mutimukwe et al., 2020; Trüdinger and Steckermeier, 2017). However, the literature overlooks the fact that control is also relevant at the organisational level, as the notion of control extends beyond strictly individualistic approaches (Lazaro and Le Metayer, 2015). Lazaro and Le Metayer (2015) argue that individual control cannot be exercised without the organisation putting a 'control architecture' in place. Such an architecture, they posit, would consist of a regulated set of structural measures that aim to secure an individual's personal data, i.e., technological controls and organisational controls. Control can also refer to the dynamic of 'power' over data (Johnson, 2009), a power which Laczniak and Murphy (1993) define as 'the ability to control'. Control has even been used to describe the legal concept of information ownership (Baron, 2012). Information ownership refers to the possession of, and responsibility for, information, and implies control over that information (Chisholm, 2011). When privacy control fails, this leads to a privacy incident, which is defined as the loss of control, compromise, unauthorised disclosure, or unauthorised acquisition (DHS, 2017, p. 8). The key control theories (Fried, 1984; Moor, 1997) in the privacy literature are the restricted access/limited control theory (Tavani, 2008), social contract theory (Martin, 2012; Martin, 2016; Wright and Xie, 2019), and agency theory (Xu et al., 2012; Pavlou et

al., 2007). The key control theories in the nonmarket literature are those 'motivated by profit/competitive advantage' (Garriga and Mele, 2004), i.e., shareholder/stockholder theory and agency theory. These control theories are discussed below.

Restricted Access / Limited Control (RALC) Theory

The restricted-access/limited-control (RALC) theory (Moor, 1997) maintains that the best way to protect privacy is to ensure that the right people have access to relevant information at the right time, giving individuals as much control over personal data as realistically possible. RALC considers that privacy is achieved if one is able to limit and restrict others from access to personal information and personal affairs (Tavani, 2008, p. 142). RALC is not realistic in a computerised or digitised world where information is "well greased and slides rapidly through computer systems" (Moor, 1997, p. 31), and where organisations need to exercise a minimum level of control over information in order to ensure compliance with privacy legislation.

Social Contract Theory

The social contract theory (SCT) assumes that individuals will enter into a social contract with an organisation once they perceive that the benefits of this relationship outweigh the risks (Donaldson and Dunfee, 1999). Consumers form contracts based on their perceptions about firms' contractual obligations. The social contract theory of privacy maintains that privacy is governed by social contracts directing how organisations use individuals' data according to social norms (Martin, 2012; Martin, 2016), and that individuals have some level of control over that use (Bélanger and Crossler, 2011). These norms include not only the type of information expected, but also who will be able to see and use the information as well as the transmission principles associated with the information (Nissenbaum, 2009). The social contract (and consequently trust) is breached if a consumer perceives that a particular organisation has failed to meet its obligations or has failed to deliver on the

contractual agreement (Malhotra et al., 2017). Violation of the contract can also occur if the owner of the information is unaware that certain information is being collected, if the organisation sells/rents the information to a third party without consent or if the organisation uses the information in any way not consented to by the owner (Phelps et al., 2000). Consumer privacy concerns can be viewed through this theory as an outcome of the violation of perceived contracts between consumers and organisations. SCT has been leveraged in a number of information privacy studies (for example, Bansal et al., 2010; Li et al., 2010; Martin, 2016; Okazaki et al., 2013; Wright and Xie, 2019).

Agency Theory

The agency theory view of privacy relates to the relationships and issues arising between principles and agents (Eisenhardt, 1989) such as the agent pursuing their own interests as opposed to the principles. Xu et al.'s (2012) study of privacy assurances used agency theory to distinguish between personal control and proxy control, with the organisation increasingly becoming the 'control agent'. These concepts locate control either with the individual where 'the self acts as the control agent to protect privacy' or the organisation where 'powerful others … act as the control agents to protect privacy' (Xu et al., 2012, p. 1346). Extant research suggests that for organisations, control-based privacy activities focus on privacy as a risk management/compliance exercise, for example, by legally selling/sharing personal data but without sharing value with the individuals supplying it (Greenaway and Chan, 2013). It seems reasonable to therefore suggest that control-based privacy activities will most likely benefit the organisation and focus on regulatory compliance.

Shareholder/Stockholder Theory

In the traditional view of the firm or the shareholder view, the shareholders or stockholders are the powerholders of the organisation, and the organisation has a binding fiduciary duty to put their needs first, so as to increase value. In the agency theory view of the organisation, the agent (typically the employee or organisation) is motivated by extrinsic rewards, for example, ensuring shareholder values (Garriga and Mele, 2004) and power is institutionally directed (Garriga and Mele, 2004). The traditional understanding of CPA amongst scholars was through the lens of shareholder theory, which assumes that organisations engage in CPA to advance policies that will benefit the firm (Hadani et al., 2105) by improving performance and delivering higher returns to stockholders. However, organisations can be led by managers who behave opportunistically and use the resources available in the organisation to pursue their own personal political agenda. Thus, agency theory became a more influential theoretical perspective applied in CPA research (Mellahi et al., 2016; Schillemans and Busuioc, 2015).

2.3.2 Theories of Justice

Kolm (1997) defines justice as the central ethical judgment regarding the effects of society on the situation of social entities. Justice is the primary standard by which social and political structures, actions, and practices are evaluated (Kolm, 1997). The extent to which individuals are treated fairly regarding their personal information is an important determinant of justice perceptions (Ashworth and Free, 2006). Individuals make such judgments regarding fairness by comparing their treatment to normative standards, referred to as prescriptive norms (Cialdini and Trost, 1998). In privacy, these prescriptive norms are reflected in a variety of guidelines articulated by a number of different regulatory bodies (Ashworth and Free, 2006) such as Fair Information Privacy Practices (FIPPs). FIPPs are a

series of discretionary principles, namely transparency, preference, purpose, minimisation, limitation, quality, integrity, security, and accountability (DHS, 2018).

Organisations that explicitly apply FIPPs are more likely to retain consumers and gain an advantage over competitors (Culnan and Armstrong, 1999) and benefit from a greater willingness to transact business (Culnan and Bies, 2003). Bonner and Chiasson (2005) highlight how FIPPs play multiple roles in privacy research. These include FIPPs as a means of assuring individual control over information, as an objective standard for assessing individual concerns about privacy (Culnan and Armstrong, 1999; Smith et al., 1996), and as an ethical standard for corporate behaviour (Culnan and Bies, 2003).

Justice is not new to privacy research and several privacy studies have applied justice-based frameworks (e.g., Ashworth and Free, 2006; Greenaway et al., 2015; Henle et al., 2009). Organisational justice refers to perceptions of fairness in decision-making and resource allocation (Greenberg, 1987). An organisation's control over personal information is considered 'just' by the consumer, when the consumer is vested with the key principles of FIPPs (Culnan and Bies, 2003; Greenaway et al., 2015). Justice-based theories in the nonmarket literature are those 'motivated by expressing the right thing to do' (Garriga and Mele, 2004), i.e., stewardship theory and stakeholder theory. According to Aguilera et al., (2007), a CSR policy meets stakeholder need for fairness and perceived organisational justice. Moreover, responses to CSR activities have been found to influence perceptions of organisational justice and fairness (Collier and Esteban, 2007; Galbreath, 2010). CSR activities are likely to demonstrate that an organisation endorses the principle of fairness, and therefore heighten an individual's perception of organisational justice.

Organisational justice comprises at least three dimensions, namely distributive, interactional and procedural justice (Colquitt, 2001; Colquitt et al., 2012). One can view justice as a lifecycle of how the consumer interacts with an organisation. Distributive

justice explains the evaluation of costs and benefits made by the consumer before deciding on the transaction. Interactional justice follows, to explain the actual decision to transact. Finally, the lifecycle concludes with procedural justice where the consumer believes that their transaction has been processed fairly. These three dimensions of organisational justice theory, i.e., distributive, interactional and procedural, paired with stewardship theory and stakeholder theory, are discussed below.

Distributive Justice Theory (DJT)

DJT reflects the perceived fairness of decision outcomes (Homans, 1961) such as comparing costs and benefits derived from disclosing personal information. Perceptions of distributive justice also involve a social comparison process (Adams, 1965), comparing benefits from different organisations for the same personal information. Kolm (1997) holds that questions of distributive justice arise when the issue is how to arbitrate among competing claims by opposing groups. For example, competing claims between employer and employee, or between consumer and organisation. Many privacy theories and practices can be understood from a process-distributive perspective (Johnson, 2016), where privacy is protected to the extent that transfers of information are limited to those permitted under some principle of justice during the transfer, for example, in corporate privacy policies where informed consent is the implied principle of justice (Johnson, 2016). The principle behind a publicly available privacy policy is that via transparency, consumers can understand the collection and use of their information and decide on their course of action. Judgements of distributive justice reflect consumers' evaluations of the fairness of the allocation of outcomes (Ashworth and Free, 2006) and have been used in studies to explain privacy risk (Xu, 2009) and privacy concerns (Zhou, 2015). Distributive justice has also been applied to construct a framework for distributing workplace surveillance privacy between the organisation and the individual so that it is fair (Introna, 2000).

Interactional Justice

Interactional justice broadly refers to the fairness of the interpersonal treatment that people receive during the enactment of procedures. Research suggests that people react strongly to the quality of interpersonal treatment, where the nature of the treatment they receive from others acts as a determinant of fairness (Greenberg, 1993). The interactional factor helps to explain why some customers feel unfairly treated even though they would characterise the procedure and outcome as fair. For example, fair treatment is characterised by the consumer's perception of an organisation honouring statements made in its privacy policy such as not to contact the customer with promotional offers or not to share customer information with third parties (Lwin et al., 2016). Interactional justice turns attention to the importance of the interpersonal treatment people receive when procedures are implemented, and reflects the perceived fairness of the treatment received from another party (Bies and Moag, 1986). Bies (1993) identifies a variety of interactional factors that might shape consumer privacy concerns such as honesty and the fulfilment of promises, or the unwarranted disclosure of personal information. Trust and respect are also important aspects of interactional justice (Turel et al., 2008). When users believe that organisations are trustworthy and honest in their compliance with promises to protect information privacy (Son and Kim, 2008), they have less privacy concerns (Zhou, 2015).

Procedural Justice Theory (PJT)

PJT, also known as procedural fairness, posits that individuals will disclose personal information if they believe there are fair procedures in place to protect their information (Culnan and Armstrong, 1999). PJT affects the perceived fairness of processes (Thibaut and Walker, 1975) and how they are enacted and communicated (Leventhal, 1980). Lind and Tyler (1988) argue that procedures also convey the extent to which individuals are respected and valued, which they call the relational or group-value model of procedural justice. A central element of PJT is the control over information disclosure, or what has

been referred to as "voice" in organisational justice research (Greenberg and Folger, 1983), allowing consumers to make informed choices. PJT emphasises the extent to which organisations offer transparency to their customers (Greenaway et al., 2015) thus building trust, and reducing consumer privacy concerns (Culnan and Armstrong, 1999). PJT has been used to explain consumer privacy concerns (Ashworth and Free, 2006; Culnan and Bies, 2003), perceptions of privacy invasion (McNall and Stanton, 2011), perceptions of fairness (Eddy et al., 1999), perceptions of privacy needs (Callan, 2018), and privacy compliance intentions (Son and Park, 2016). It seems reasonable to suggest that justice based NMPv activities will most likely benefit the individual and focus on fairness and ethics. Several privacy studies have linked PJT with FIPPs (Ashworth and Free, 2006; Culnan and Armstrong, 1999; Culnan and Bies, 2003; Greenaway et al., 2015).

Stewardship and Stakeholder Theory

Most often the literature applies stakeholder theory to determine and explain Corporate Social Responsibility's effect on firm performance (e.g., Chang et al., 2014; Madsen and Rogers, 2015). By representing the needs of all stakeholders, stakeholder theory identifies how traditional boundaries between nonmarket strategies have become blurred, so that certain types of CPA, which resemble Corporate Social Responsibility, emerge. These types of CPA are referred to as 'deliberative lobbying' (Lock and Seele, 2017). Certain types of CSR resembling CPA also emerge, such as Political CSR (e.g., Matten and Crane, 2005; Scherer and Palazzo, 2011; Scherer et al., 2016). Given this potential synergy between CPA and CSR, researchers recommend integrating stakeholder and stewardship theories (Laplume et al., 2008; Preston 1998) and therefore both are combined in this section.

Stewardship theory (Donaldson and Davis, 1991) suggests that a firm's purpose is to contribute to humanity by "serving customers, employees and the community" (Karns, 2011, p. 337). At the centre of the theory's foundation is the concept that organisations are

here to serve rather than make a profit. However, to be able to serve, they must sustain themselves financially. The stewardship theory states that a steward protects and maximises shareholders wealth through firm performance. Stewards are assumed to be motivated to act in the best interests of their principals (Davis et al., 1997). Stewardship theory is involved mainly in analysing the importance of the co-existence of trust-based relationships along with agency relations in firms (Balakrishnan et al., 2017). While early views of stewardship focused on managers as stewards of the firm, with their own survival needs (Davis et al., 1997) there has been a shift to 'ethical stewardship' which emphasises individuals at different levels (for example, owners, managers and employees) adopting prosocial values and behaviours and socially contracted relationships (Caldwell and Karri, 2005). These social contracts (Donaldson and Dunfee, 1999) extend from the firm to other levels of society, such as the industry or community (Hernandez, 2012). Ethical stewardship is defined as a theory that integrates long-term wealth creation, a commitment to the transformational interests of stakeholders, and creating organisational systems that reinforce both instrumental and normative organisational goals (Caldwell et al., 2008, p. 154).

Boatright and Peterson (2003) affirm that organisations are operated for the benefit of all those who have a stake in the firm. For example, shareholders invest their money in enterprises, employees invest their time and intellectual capital, customers invest their trust and repeated business, and communities provide infrastructure and education for future employees (Boatright and Peterson, 2003). The stakeholder theory (Freeman, 1994) perspective in the nonmarket environment assumes that organisations should consider the rights of multiple stakeholders including governmental bodies, political groups, trade associations, trade unions, financiers, suppliers, employees, customers, suppliers, and local communities etc. Even competitors are counted as stakeholders due to their capacity to affect the firm and its other legitimate stakeholders (Spence et al., 2001). Stakeholder-

based decision making requires a balancing of these interests. Stakeholder theory can be considered a CSR theory (Melé, 2008) that can be usefully applied in CSR practice (Hörisch et al., 2014). Pérez and del Bosque (2016) use stakeholder theory to explore customers' multidimensional perceptions of organisations and their CSR orientations, finding that customers' perceptions of customer-related CSR and broad legal and ethical issues have a significant positive impact on customer satisfaction.

2.3.3 Theories Combining Control and Justice

As discussed, privacy is dynamically changing depending on context and time. Essentially control and justice become two dynamic forces in motion, responding to dynamic needs for privacy across context and time. Individuals and organisations both have needs to control privacy of information and when one party's control needs are met, they perceive this as fair. However, the other party may not. Therefore a theory that represents negotiating the balance or exchange of control or justice is beneficial. Two theories in the literature that reflect this concept of balance or exchange, are Social Exchange Theory (SET) (Blau, 1964) and the PRE theory (Davis et al., 1980).

In nonmarket environment literature, CSR and SPI have obvious relationships with justice theories, and CPA is clearly linked with control theories. However, SET and power relations theory have been used to explore both strategies. SET (Blau, 1964; Emerson, 1976) has been used to explore the possible interactions between CPA and CSR by positioning the business–government relationship as an ongoing social exchange (Du et al., 2019). SET has also been used in the nonmarket environment context, to explain organisational commitment and employee trust (Farooq et al., 2013), and employee performance and customer service orientation (Hu et al., 2020). SET and PRE Theory are discussed in the remainder of this section.

Social Exchange Theory (SET)

SET views interpersonal interactions from a cost-benefit perspective. Whilst this is similar to an economic exchange (Blau, 1964), a social exchange deals with the exchange of intangible social costs and benefits (Gefen and Ridings, 2002). Like an economic exchange, social exchange assumes that individuals take part in an exchange only when they expect their rewards to justify the (sometimes intangible) costs of taking part. The key difference between a social and economic exchange is that a social exchange gives no guarantee that there will be reciprocal rewards in return for the costs invested (Blau, 1964) because there are no governing rules other than the assumed cooperative intentions/reciprocity of the other party (Kelley and Thibaut, 1978). Without the belief that the other party will reciprocate fairly, parties are less likely to take part in a social exchange (Blau, 1964). SET has been used to explore consumer trust production and privacy concern (Xueming, 2002), consumer trust perceptions and the willingness to share information online (Dwyer et al., 2007), and consumer promotion/prevention behaviours regarding personal information (Mostellar and Poddar, 2017).

Power Responsibility Equilibrium (PRE) theory

Like much of both the control and justice theories discussed to this point, the level of control over consumer information considered ‘just’ is often judged in these studies at the individual level, i.e., there is no consideration of the needs of the organisation or other significant stakeholders such as regulators and governments. The PRE theory (Davis et al., 1980) addresses this gap. PRE theory stems from power relationship studies and advances the balance between power and responsibility. Power is a relational concept that refers to the asymmetric control over valued resources, which in turn affords an individual the ability to control others' outcomes, experiences, or behaviours (Tost, 2015). In this way, PRE theory could be considered a control theory. However, in PRE theory, power holders are also obligated to act in a socially responsible manner due to social evaluation and

pressure (Bandara et al., 2020). In the nonmarket literature, Davis (1960) was one of the first to explore the role of power that business has in society and the social impact of this power. In doing so, Davis (1960) introduced the power responsibility equilibrium as a new element in the debate of nonmarket strategy, and refers to the approach as 'Corporate Constitutionalism' (Garriga and Melé, 2004). According to Davis, the function of power can be limited by pressures of different constituency groups who define conditions for the responsible use of power (Garriga and Melé, 2004).

In this research, power is interpreted as 'control', as power has been defined as 'control' in existing research (Anderson and Brion, 2014) and is often considered synonymous with control (Laczniak and Murphy, 1993). Justice is interpreted as responsibility, as responsibility is associated with justice (Fia and Sacconi, 2019). The PRE theory states that power should be in equilibrium, where the more powerful partner in a relationship has the societal obligation to ensure an environment of trust and confidence (Lwin et al., 2007). Accordingly, this theory suggests that the powerful member in a relationship should exhibit power and responsibility equally towards the less powerful member. When an organisation exercises high-power and low-responsibility strategies, it will lose power in the long run (Caudill and Murphy, 2000; Murphy et al., 2005), for example from increased regulation (Caudill and Murphy, 2000) or from consumers taking defensive action to reduce the organisation's power (Bandara et al., 2020; Krishen et al., 2017; Lwin et al., 2007). In PRE, power holders are expected to exhibit felt equality with less powerful partners. The inability to do so will result in forces curtailing power, demanding more responsible actions, or both, to maintain an equilibrium. In a balanced-power relationship, individuals will treat others as equals, be more concerned about the welfare of others and give benefits to others non-contingently (Schaerer et al., 2018).

Developed on the PRE theory, the PRE Model of Privacy (Lwin et al., 2007), outlined in Figure 2.3, holds that consumers who perceive that organisations are acting responsibly in

terms of their privacy practices, are expected to have greater trust and confidence in organisations and show less concern for privacy (Lwin et al., 2007). Lwin et al. (2007) classify organisations and government on one side, i.e., the powerholders who are expected to show responsibility. They classify consumers on the other side, i.e., the information providers who expect responsible use of control/power. Consumers will take defensive actions when corporations and governments fail to promote equality in an information exchange and effectively manage privacy protection. These consumer actions are driven by deficits in privacy protection by powerholders (Bandara et al., 2020; Caudill and Murphy, 2000; Krishen et al., 2017; Lwin et al., 2007).

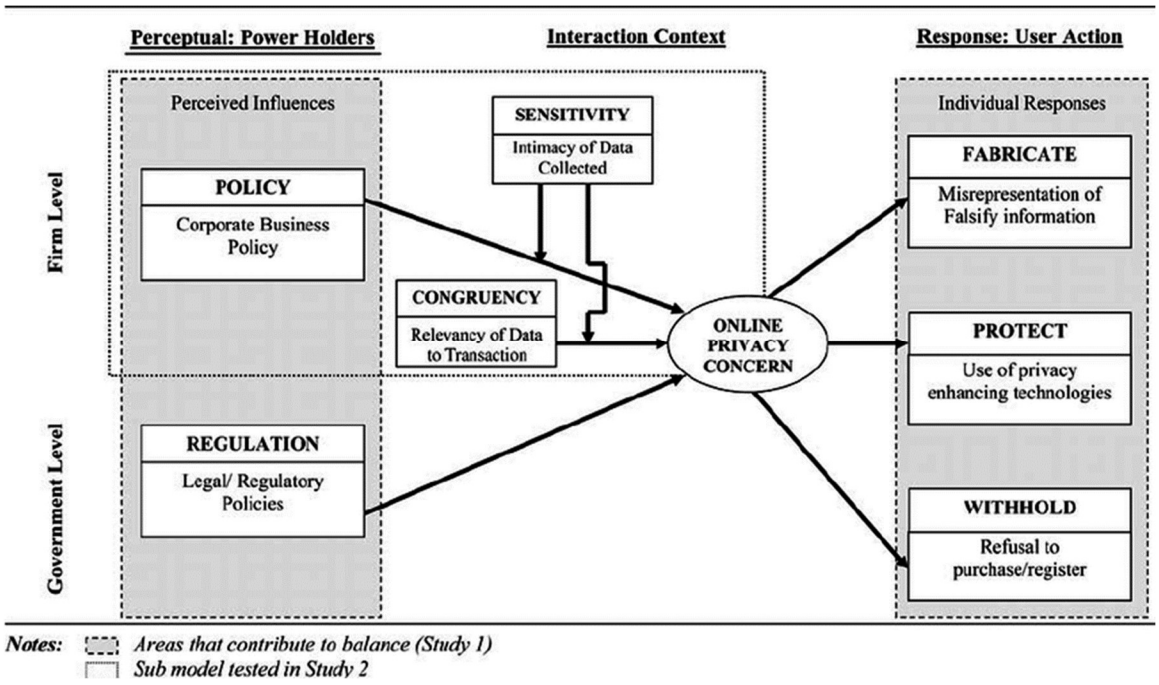


Figure 2.3 The PRE Model of Privacy

(Source: Lwin et al., 2007)

If organisations are not seen to be responsible, privacy concern is likely to increase, leading to defensive measures by consumers (Liedong et al., 2014) or measures by other stakeholders, such as regulators. Facebook and Google, for instance, have both been instructed by the FTC to conduct independent privacy audits for the next 20 years as a result of repeatedly not offering responsible privacy practices (Forbes, 2011). Inversely,

where an organisation is seen to have consumer-friendly privacy practices, they are perceived as responsible, and thus will lessen privacy concern (Caudill and Murphy, 2000). Krishen et al. (2017) extended the PRE Model of Privacy (Lwin et al., 2007) to include individual differences, i.e., locus of control, and cognitive responses, i.e., fairness and attitude towards marketing communications. More recently, Bandara et al. (2020) extend consumer responses in the PRE Model of Privacy to include consumer trust, and extend powerholders to include not only the corporate policy of the organisation but also their corporate privacy responsibilities. Bandara et al. (2020) define corporate privacy responsibility as the organisation's responsibility to incorporate not only legal responsibilities, but also ethical responsibilities into their data privacy management practices.

PRE does not presume that only one party can be the powerholder, although the literature most often presumes the organisation as such. For instance, as per Lwin et al. (2007), governments and regulators are the powerholders over organisations. Other possible powerholder combinations could be shareholders over organisations, employers over employees etc. PRE also recognises that legislation may affect the level of power that an organisation can exercise over privacy (Lwin et al., 2007). For instance, the stringency of GDPR over privacy has restricted the use and collection of data, thus reducing the power that organisations have to extract utility from this information. Most importantly, GDPR introduced the concept of statutory data subject rights for the first time. These rights enable a data subject to have powers such as GDPR's right to be deleted. This results in customers becoming powerholders on one side, by demanding deletion of their data, whilst organisations on the other side have legitimate needs to retain data in line with predetermined schedules. Thus, this research proposes that privacy be considered an exchange, between not just two but several parties, in which all parties needs for control

are considered so that the outcomes are 'just' for all involved parties. Balance is achieved when both the individuals and organisations expectations are met (Kucuk, 2016).

2.4 The Nonmarket Environment

As this research is focused on exploring privacy activities in the nonmarket environment, a number of definitions are presented here to help understand the differences between the nonmarket environment and the market environment. This is followed by a discussion of the key strategies that organisations apply in the nonmarket environment, and the approaches that organisations take towards those strategies.

2.4.1 The Market Environment and Nonmarket Environment

The market environment is defined as the interactions between the firm and other parties that are intermediated by markets or private agreements (Baron, 1995). In this environment, organisations typically compete for resources and revenues (Doh et al., 2012; Wrona and Sinzig, 2018) and undertake interactions that *directly* shape profitability, such as lowering costs, increasing prices or revenue, marketing and advertising, and enhancing response times. In contrast, the nonmarket environment is defined as those interactions between the organisation and other parties that are intermediated by the public, stakeholders, government, the media, and public institutions (Baron, 1995). In the nonmarket environment, organisations undertake interactions that *indirectly* shape profitability, such as advising public policy, working with activists, influencing regulators, influencing governments, managing media, and building coalitions.

The nonmarket environment differs from the market environment in several important respects. First, the market environment consists mainly of suppliers, customers, and

competitors. The nonmarket environment, by contrast, can be characterised primarily by the social, political, legal, and cultural arrangements that constrain or facilitate organisational activity or behaviours (Funk and Hirschman, 2017). Second, in the market environment, organisations typically compete for resources, revenues, and profits. Whereas in the nonmarket environment, organisations consider broader dimensions of impact and performance such as ethical behaviour, policy attainment, and social responsibility (Doh et al., 2012). Third, in the nonmarket environment, organisations compete not just with private interests within their industries or across other industries, but also with political and social actors. Where the primary means of exchange between an organisation and its market actors is money, which directly impacts revenue and costs, the primary means of exchange between an organisation and its nonmarket environment actors is information, which indirectly impacts revenue and costs (Liedong et al., 2014).

How an organisation interacts with its market environment is referred to as its 'market strategy'; how it interacts with its nonmarket environment is referred to as its 'nonmarket strategy' (Baron, 1995). Market strategy is defined as a concerted pattern of actions taken in the market environment to create value by improving the organisation's economic performance (Baron, 1995). A market strategy consists of a set of market actions, such as pricing reviews, new product development, product diversification, innovation, international expansion, and research and development investments (Ozer and Alkent, 2012). Market strategies aim to maximise performance by first identifying opportunities, then developing, exploiting, and sustaining the competitive advantage required to pursue those opportunities (Baron, 1995). In contrast, nonmarket strategy is defined as an organisation's activities aimed at improving its performance by managing the competitive environment (Baron, 1995; Lux et al., 2011; Voinea and van Kranenburg, 2018). A nonmarket strategy consists of a set of nonmarket actions such as building coalitions, lobbying legislators or regulators, making campaign contributions, and providing

information to affect institutions that might defend or create revenues (Doh et al., 2012). Nonmarket strategies aim to maximise overall profits by participating in the public processes leading to the resolution of nonmarket issues (Voinea and van Kranenburg, 2018).

Both market and nonmarket strategies can provide a competitive advantage relative to market rivals, but nonmarket strategies can also establish or enhance an organisation's competitive advantage (Liedong et al., 2014; Lawton et al., 2013) by enabling entry into new markets, reducing regulation, disabling rivals, limiting price increases, and raising the costs for competitors (Liedong et al., 2014). Nonmarket strategies can also provide a direct advantage that benefits all organisations in an industry, for example by reducing the costs of industry members (Bach and Allen, 2010). Whilst profitable return cannot be assumed for nonmarket strategies, participants beyond the market have a significant influence on an organisation's competitive position (Bach and Allen, 2010). Thus, there is an overlap between market and nonmarket strategies (Doh et al., 2012) whereby both create and sustain competitive advantage (Porter and Kramer, 2011). As noted in Section 1.3.1, the two predominant strategies in the nonmarket environment are CSR and CPA (Doh et al., 2012; Lawton and Rajwani, 2015), with SPI an emerging nonmarket strategy (Nalick et al., 2016). Table 2.1 outlines key definitions for these three nonmarket strategies.

Table 2.1 Definitions of Nonmarket Strategies

Nonmarket Strategy	Definition	Author(s)
Corporate Social Responsibility	Actions that further some social good beyond interests of the firm and beyond that which is required by law.	McWilliams and Siegel (2001)
	An evolving umbrella term for a variety of concepts and practices, which recognise that organisations have a societal responsibility towards privacy beyond legislation and liability.	Blowfield and Frynas (2005)
	Actions an organisation can take that contribute to social welfare, beyond those required for profit maximisation. These cover a wide range of issues, such as employee relations, human rights, corporate ethics, community relations, and the environment.	McWilliams (2015)
	A type of international private law - a socio-political movement which generates private self-regulatory initiatives, incorporating public and private international law norms seeking to ameliorate and mitigate the social harms of and to promote public good by industrial organisations.	Sheehy (2015)
Corporate Political Activity	Efforts made by organisations to influence government policy in ways favourable to them.	Hillman et al. (2004)
	Corporate attempts to influence legislative/regulatory processes and outcomes.	Anastasiadis (2014)
Sociopolitical Involvement	An organisation's public demonstration of support, i.e., statements or actions, for or against a wide array of partisan sociopolitical issues, with no direct performance motivation.	Nalick et al. (2016)

In the remainder of this section, approaches to these nonmarket strategies and differences between them are discussed. This will help form the foundations to address *RQ2: Can an organisation's approach to nonmarket privacy be determined from their published nonmarket privacy activities?*

2.4.2 Corporate Social Responsibility (CSR)

CSR is often used interchangeably with the terms corporate sustainability, corporate responsibility, corporate citizenship, sustainable development, corporate sustainability, and the triple bottom line (Montiel, 2008; Sheehy and Farneti, 2021). Although these variations

in terminology leave CSR having 'unclear boundaries and debatable legitimacy' (Lantos, 2001, p. 1), they stem in part from differing fundamental assumptions about what CSR entails and how CSR is embedded into the organisation (Jamali, 2008). CSR has evolved from concepts of minimal legal and economic responsibilities (Carroll, 1979) to broader responsibilities towards the wider social system such as public responsibilities and social responsiveness (Wartick and Cochran, 1985). In his CSR pyramid, Carroll (1979, 1991) categorises CSR into four pillars arguing that making a profit, within the boundaries of the law, is the quintessential responsibility of organisations, after which organisations can consider their ethical and philanthropic responsibilities. The philanthropic and ethical component of Carroll's CSR Pyramid are often considered to be the roots of CSR (van Marrewijk, 2003; Carroll and Buchholtz, 2003). Concepts of CSR evolved over time in response to changes in the market environment and advancing concerns of the wider stakeholder community regarding competitiveness and reputation (Carroll, 2016; Latapi-Agudelo et al., 2019). These concerns and CSR practices have given rise to the emergence of four discrete perspectives of Corporate Social Responsibility, namely stakeholder, strategic, political and shared value.

The stakeholder theory of CSR (Freeman, 2001) extends Elkington's (1999) Triple Bottom Line concept. This concept emphasises how in order to be sustainable, organisations need to measure not only their financial performance, but also measure their impact on the extended stakeholder community, including the broader economy, the environment, and the society in which they operate (Savitz, 2013). According to the stakeholder theory of CSR, the organisation should be used as a vehicle for coordinating stakeholder interests instead of maximising shareholder profit (Freeman, 2001). Definitions of CSR as responsibilities towards society emerged, where organisations have obligations to the society they are an integral part of (van Marrewijk, 2003; van Marrewijk and Were, 2003). Van Marrewijk (2003) suggests that CSR refers only to an organisation's activity that

demonstrates the inclusion of social and environmental concerns in business operations and in interactions with stakeholders.

Lantos (2001) extends the stakeholder theory of Corporate Social Responsibility, to highlight CSR as a strategic tool. CSR could become a strategic tool when part of the organisation's management plans or an organisation takes part in activities that can be framed as socially responsible, albeit only if these actions result in financial returns (Lantos, 2001). Chandler and Werther (2013, p. 65) defined strategic CSR as: "The incorporation of a holistic CSR perspective within a firm's strategic planning and core operations so that the firm is managed in the interests of a broad set of stakeholders to achieve maximum economic and social value over the medium to long term." The primary objective of strategic CSR is to gain a market advantage by aligning the organisations needs with its consumers values to ensure positive consumer reactions. (Kuokkanen and Sun, 2020).

This focus on stakeholders and the strategic power of Corporate Social Responsibility led to the identification of other important and influential stakeholders, such as government and polity, with several studies highlighting CSR as a broad 'political' responsibility (e.g., Maier, 2021; Matten and Crane, 2005; Mellahi et al., 2016; Scherer and Palazzo, 2011). Organisations thus began to adopt CSR activities that increased their role in governance at a national or global level (Detomasi, 2008). By leveraging their CSR activities, organisations engaged in 'self-regulation', where existing governance mechanisms had failed or were found to be inefficiently enforced (King and Lenox, 2000; Maxwell et al., 2000). In this context, CSR activities, such as philanthropic donations and sponsoring activities, were used to gain access to political elites (Fooks et al., 2013) and bridge governance gaps (Gond et al., 2011).

Thus, a growing body of literature termed ‘Political Corporate Social Responsibility’ emerged, examining how organisations used CSR to affect policy outcomes by influencing political constituencies (Fooks et al., 2013). Political CSR (Maier, 2021; Scherer, 2018; Scherer and Palazzo, 2011) emphasises the state-like role of multinational corporations, distinguishing political CSR from the instrumental approaches that focus on the business case of CSR (Scherer, 2018), and focuses on a firm's assumption of governmental roles and responsibilities in a global context, in which weak governance may prevail (DenHond et al., 2014). The use of Political CSR to gain political leverage was found to reduce the risk of unfavourable regulation (McDaniel and Malone, 2012; Tesler and Malone, 2008) and improve the overall business climate (Dorfman et al., 2012; Maier, 2021).

Porter and Kramer (2011) then shifted the discussion around CSR towards the concept of creating shared value, explaining it as a necessary step in the evolution of business. They define the concept as the policies and operating practices that enhance the competitiveness and social conditions of the communities in which an organisation operates. Latapi-Agudelo et al. (2019) argue that whilst Porter and Kramer (2011) did not contribute directly to the concept of CSR, they called for a change in business strategies to focus on generating shared value as a main objective. In 2013, Chandler and Werther partnered strategic CSR with the concept of creating shared value, claiming that the first step towards strategic CSR was to identify the social problems for which the organisation can create a market-based solution in an efficient and socially responsible way. Chandler (2016) suggests that organisations should aim at optimising value over the long term by focusing on their core expertise, resulting in a re-orientation of efforts towards creating shared value instead of profit maximisation.

There are two key approaches to CSR in the literature: CSR Generations from Trapp (2012) and CSR Postures from Castello and Lozano (2009). The term ‘approach’ is described by Trapp (2012) as an organisation’s understanding of Corporate Social

Responsibility, its CSR program development, and CSR communication. Trapp (2012) proposes a three-generation approach to Corporate Social Responsibility. In First Generation, organisations refrain from illegal activities. In Second Generation, organisations secure rights for employees, their families, and local communities. Finally, in Third Generation, CSR is driven by concerns that surpass legal and stakeholder interests and involve understanding the complex interconnections between corporate activities and the greater global context (Trapp, 2012). Castello and Lozano (2009) refer to approaches to CSR as 'postures' and describe three CSR postures, namely; Risk Management Posture, Integrated Posture and Citizenship Posture. According to Castello and Lozano (2009), the Risk Management posture sets compliance as the goal, where governance is assigned to functional management and neither vision nor mission are related to CSR activities. The Integrated Posture offers robust compliance to regulation as a baseline, whilst recognising and minimising the limitations of bare compliance. The Citizenship Posture is focused on building and maintaining sustainable relationships by reaching out to stakeholders and associating their CSR activities with other strong values such as trust and integrity (Mirvis and Googins, 2006). Table 2.2 presents an overview of CSR Postures from Castello and Lozano (2009).

Table 2.2 Approaches to Corporate Social Responsibility (CSR Postures)

(Source: Adapted from Castello and Lozano, 2009)

CSR Posture	Characteristics/Perspectives
Risk Management	• CSR programs undeveloped. CSR is considered a tool to protect reputation • CSR-related policies and activities focus on the firm's activities with the highest risk potential • CSR policies and practices focus on compliance with laws and industry standards • Compliance and governance is assigned to the functional department managers • Neither the firm's strategic positioning, vision or mission are related to the CSR activities
Integrated	• Awake to society's increasing expectations, firm changes their business models to include social responsibilities • Report on company values towards societal expectations and reflection on how social issues can gain competitive advantage • Aim is to mitigate economic loss medium term and achieve longer-term gains by daily responsible practices • CSR activities are proactive and systematic, strategic rhetoric reflects CSR values through slogans, marketing • Often using standards such ISO 26000 or Global Reporting Initiative • Top management are assigned to CSR programs, strong internal leadership • Relationships with stakeholders evolve from one-way communication to dialogue and collaboration
Citizenship	• Reach out to stakeholders, incorporate social issues as values held strongly by the firm • Associate CSR with other strong values such as trust and integrity, assume a citizenship role leading social issues and transforming their business models to achieve this objective • Broaden their agenda by expanding their social concerns and deepening the involvement of top management in the leadership of change regarding social issues • Form long-term strategic alliance and partnerships with stakeholders in order to drive change in social issues • Stewardship role – top management generate commitment from other stakeholders

An alignment between CSR Generations (Trapp, 2012) and CSR postures (Castello and Lozano, 2009) emerges, in which the First Generation CSR is consistent with a Risk Management Posture, the Second Generation CSR is consistent with an Integrated Posture, and the Third Generation CSR is consistent with a Citizenship Posture.

2.4.3 Corporate Political Activity (CPA)

In many industries, the success of business in shaping government policy is no less important than business success in the marketplace. As a result, it is critical for organisations to develop corporate political strategies as a part of their overall nonmarket

strategy (Baron, 1995; Oberman, 1993). Oliver and Holzinger (2008) describe CPA as strategic political management, i.e., a set of strategic actions that firms plan and enact for the purpose of maximising economic returns from the political environment. Baron (1995, p. 47) argues that CPA is an important part of the firm's nonmarket strategy that constitutes a "pattern of actions taken in the nonmarket environment to create value by improving its overall performance". CPA typically aims to achieve favourable outcomes and competitive advantage for organisations (Baysinger, 1984; Hadani, et al., 2018). CPA is considered part of an organisations right to speak on public issues and protect their interests (Lascelles, 2005; Ostas, 2007). For instance, the right to lobby or petition the government is included within the right to free speech (Redish, 1982; Allard, 2008).

Hillman and Hitt (1999) identify three key pillars of CPA, namely constituency building, financial incentives and information strategy. Constituency building helps to form strong coalitions and public support for policy influence (Baysinger and Butler, 1985; Lord, 2000), while financial incentives provide monetary inducements to political decision makers meant to sway them towards the interests of donating firms. Examples include political action committee (PAC) contributions and political directorships (Milyo et al., 2000). Information strategy entails using information to shape policy decisions, where tactics include lobbying, research reports, and press conferences. The literature typically considers lobbying and CPA as synonyms (e.g., Anastasiadis et al., 2018; Doh et al., 2012; Lawton et al., 2013; Lux et al., 2011; Wrona and Sinzig, 2018) and the terms are used interchangeably in this thesis. Lobbying occurs when an organised interest provides information to a policy maker in hopes of influencing the decision-making process (Anastasiadis et al., 2018; Rudy and Cavich, 2017).

CPA is typically more focused on the corporate good than the common good (Liedong et al., 2014) with organisations often participating in CPA as a reaction to issues that directly affect only themselves (Hadani et al., 2018). This perception may, however, be unfair as

organisations are in fact corporate citizens (Moon et al., 2005; Richter, 2011; Wood and Logsdon, 2008) that have sometimes played political roles to ensure the common good and social welfare (Liedong et al., 2014). Additionally organisations may have knowledge that is useful for policy making (Hamilton and Hoch, 1997) and by sharing this knowledge, they help politicians understand issues from different perspectives and enable them to formulate informed policies that benefit society while reducing unintended consequences (Christensen et al., 2017; Lawton et al., 2014).

Where CPA is judged by what private returns it brings to the organisation, it is termed 'instrumental CPA' or 'instrumental lobbying' (Lock and Seele, 2017). Influencing the nonmarket environment contributes to firm performance, whether economic or reputational. Improvement of the bottom line is arguably the end goal of CPA, where organisations' political engagements and manoeuvres shape their competitive space and enable them to exploit economic opportunities (Capron and Chatain, 2008; McWilliams et al., 2002). Researchers and practitioners have proposed alternatives to instrumental lobbying, such as ethical lobbying (e.g., Gao, 2008) or responsible lobbying (United Nations Global Compact, 2005; Baron, 2008). Building on the transformative concept of Political CSR, Lock and Seele (2017) describe this concept of ethical/responsible lobbying as 'deliberative lobbying' and define it as an organisation's understanding of its ethical or responsible role in the political process. Deliberative lobbying, they posit, is based on disclosure, transparency, choice, and accountability that aims to resolve public issues, and aligns CSR and CPA strategies (Lock and Seele, 2017). Deliberative lobbying is not unlike Political CSR, which refers to activities beyond traditional CSR programs, where organisations are placed in quasi-governmental roles (Valente and Crane, 2010).

There is mixed opinion on the relationship between CPA and performance outcomes for the organisation. CPA is often positively associated with increased performance outcomes (Rajwani and Liedong, 2015; Wrong and Sinzig, 2018). These outcomes have been argued

to occur as a result of reducing uncertainty in the nonmarket environment (Hillman and Hitt, 1999), influencing government officials to enact laws which help the organisation (Peltzman, 1976; Stigler, 1971), managing risk associated with the organisation's resource dependence (Blumentritt, 2003), or developing key relationships with government officials that result in improved competitive conditions for the organisation (Clawson et al., 1998). However, a host of scholarship finds little performance effects associated with CPA (e.g., Ansolabehere et al., 2004; Hadani and Schuler, 2013; Hersch et al., 2008). In their review of the nonmarket strategy–performance relationship, Mellahi et al. (2016, p. 147) noted that the nature of the link between CPA and performance remains elusive, as more than half of the CPA studies they reviewed between 2010 and 2014 did not find a positive relationship (Rudy and Cavich, 2017).

Approaches to CPA are defined as the manner in which an organisation engages in lobbying activity (Anastasiadis, 2014). Based on their review of the nonmarket and corporate political strategy literature, Voinea and van Kranenburg (2018) suggest that organisations can take either a transactional or relational approach to CPA (as was first proposed by Hillman and Hitt, 1999). Anastasiadis (2014), on the other hand, presents two approaches to CPA, referred to as cooperative and instrumental approaches. These differing approaches to CPA are summarised in Table 2.3.

Table 2.3 Approaches to Corporate Political Activity

	CPA Approach	Characteristics/Perspectives
Hillman and Hitt (1999)	Transactional	• Short-term strategy • Formulate CPA strategy in response to specific salient issues • Organisations await the development of an important public policy issue before formulating a strategy
	Relational	• Long-term strategy • Organisations pursue CPA strategies over the long term, rather than on an issue-by-issue basis • Organisations build relationships across issues so that when public policy issues that affect their operations arise, the contacts and resources needed to influence this policy are already in place • Trust develops between the suppliers and demanders of public policy, thereby reducing the marginal transactional costs of participation
Anastasiadis (2014)	Instrumental	• Short-term strategy • A liberal minimalist understanding of citizenship, • Based on external incentives • Illegitimate
	Cooperative	• Long-term strategy • A competent partnership understanding of citizenship • Reflects an intrinsic commitment to responsible actions • Legitimate

When organisations formulate CPA strategy in response to specific salient issues (e.g., Buchholz, 1992; Getz, 1993), this is labelled as a Transactional approach (Hillman and Hitt, 1999). In the Transactional approach, organisations await the development of an important public policy issue before formulating a strategy (Hillman and Hitt, 1999). Transactional approaches to nonmarket strategies may include issue-lobbying, temporary grassroots mobilisation of employees, suppliers, or customers, advocacy advertising, contracting media experts, press releases, and press conferences (Voinea and van Kranenburg, 2018).

Where organisations pursue CPA strategies over the long term rather than on an issue-by-issue basis, this is labelled a Relational approach (Hillman and Hitt, 1999). Instead of monitoring public interest and becoming involved only in specific issues, organisations using a Relational approach attempt to build relationships across issues and over time so that when public policy issues that affect their operations arise, the contacts and resources needed to influence this policy are already in place (Hillman and Hitt, 1999).

Transactional and Relational approaches to political action differ in terms of length and scope of continued activity and exchange (Hillman and Hitt, 1999). Such distinctions between approaches to CPA are also similarly suggested by Hadani et al. (2015) and Kroszner and Stratmann (2005), who argue that building stable relationships with public policy makers provides both sides with a chance to get to know each other and assess each other's true intentions. Hillman and Keim (1995) describe the public policy process as having 'demanders' and 'suppliers' of public policy. In a relational approach, trust develops between the suppliers and demanders of public policy, thereby reducing the marginal transactional costs of participation (Hillman and Hitt, 1999). Hillman and Hitt (1999) identify three key variables that influence the decision to adopt a transactional versus a relational approach to political action, namely (i) the degree to which organisations are affected by government policy, (ii) the level of firm product diversification, and (iii) the degree of corporatism/pluralism within the country in which the firms are operating (Hillman and Hitt, 1999). In a more recent qualitative study, however, Shirodkar and Mohr (2015) conclude that organisations operating in emerging markets increasingly implement short-term approaches, e.g., reactions to new regulations. Whereas organisations in developed markets implement long-term approaches e.g., relationship building (Shirodkhar and Mohr, 2015).

Anastasiadis (2014) argues that an organisation's basic approach to lobbying is determined by its implicit view of the nature of citizenship. The more unitary the organisation's understanding of these views, the stronger this influence. Instrumental approaches are congruent with a liberal minimalist understanding of citizenship and are considered illegitimate, whereas Cooperative approaches demonstrate competent partnership where politics and lobbying are considered legitimate (Anastasiadis, 2014).

2.4.4 Sociopolitical Involvement (SPI)

Sociopolitical issues are salient unresolved social matters on which societal and institutional opinion is split, thus potentially engendering acrimonious debate among groups (Bhagwat et al., 2020). Such issues are often partisan, yielding polarised stakeholder responses (Kotler and Sarkar 2017). Sociopolitical issues exist at intersections of time, politics, and culture and the controversy surrounding them can evolve or resolve over time (Bhagwat et al., 2020).

Although SPI is related to CSR and CPA, SPI is a relatively new phenomenon – although its nascency is already introducing conceptual ambiguity (Bhagwat et al., 2020; Hambrick and Wowak, 2021). The terms used to describe SPI differ across multiple fields of research. For example, in Marketing and Law literature, it is referred to as Corporate Social Activism (Bhagwat et al., 2020), in Business Ethics literature it is referred to as Corporate Political Advocacy (Shirodkar et al., 2018), and in Communications literature it is referred to as Corporate Social Advocacy (Dodd and Supa, 2014). However SPI generally refers to the public relations function in which organisations intentionally or unintentionally "align themselves with a controversial social-political issue outside their normal sphere of CSR interest" (Dodd and Supa, 2015, p. 288).

SPI has emerged alongside shifting societal expectations about the roles and responsibilities of business and government (Dodd, 2015). Traditionally, the public targeted government to legislate business; today, the public increasingly targets business to influence government (Dodd, 2015). Organisations are now increasingly expending resources and engaging in risk by taking public stances on issues that transcend the particular interests of a single organisation and are often aimed at societal-level outcomes (Fessman, 2016; Gaines-Ross, 2017; Vredenburg et al., 2020). Organisations participating in SPI typically undertake statements of social advocacy, such as an organisation's position on gay rights, or actions, such as the introduction of new products, the redesign of

packaging, and the creation or termination of advertising campaigns (Bhagwat et al., 2020). SPI signals an organisation's sociopolitical values, thus enabling stakeholders to evaluate the congruence of the organisation's values with their own (Miller and Triana, 2009; Vredenburg et al., 2020). Three discrete approaches to SPI emerge from the literature, namely; Corporate SPI, where the organisation takes on the role of the activist; CEO SPI, where the CEO takes on the role of activist; and Shareholder SPI, where the shareholders take on the role of activist. Definitions for these three approaches are summarised in Table 2.4.

Table 2.4 Approaches to Sociopolitical Involvement

SPI Approach	Definition	Author
Corporate SPI	An organisations public demonstration (statements or actions) of support for, or opposition to, one side of a partisan sociopolitical issue.	Bhagwat et al. (2020)
CEO SPI	A business leader's personal/public expression of a stance on some matter of current social/political debate.	Hambrick and Wowak (2021)
	Corporate leaders speaking out on sociopolitical issues not directly related to their organisation's core business.	Chatterji and Toffel (2018).
Shareholder SPI	Actions taken by shareholders with the explicit intention of influencing corporations' policies and practices.	Goranova and Verstegen-Ryan (2013)

The effect of SPI on the consumer depends on whether customers feel a sense of congruity between their values and an organisation's SPI (Bhagwat et al., 2020). The consumer's response to Corporate SPI can be shaped by their comparison of the alignment of the organisation's values with their own – and thus influence their purchase decisions (Kim et al., 2018; Swaminathan et al., 2020). Chatterji and Toffel (2018) find that CEO activism can increase consumers' intentions to purchase the organisation's products, but only to the degree that there is alignment between the CEO's message and individuals' policy

preferences. Korschun et al. (2016) find that CEO activism is viewed positively by consumers only if the organisation is considered values-oriented. The Edelman Trust Barometer highlights that the current trend towards CEOs taking the lead for sociopolitical change has increased steadily from sixty five percent in 2018 to seventy six percent 2020 (Edelman, 2020). The attention from both scholars and practitioners towards CEO activism has also risen in recent years, as more CEOs take a public stance on sociopolitical issues (McKinsey, 2020; Chatterji and Toffel, 2018; Voegtlin et al., 2019).

2.4.5 Differences Between the Key Nonmarket Strategies

While organisations have a vested interest in influencing their nonmarket environment, not all nonmarket strategies that organisations engage in are clearly salient to their overall objectives. Nalick et al. (2016) identify three key differentiating characteristics of these nonmarket strategies, namely objectives, operational relationships, and beneficiaries.

First, the objectives for engaging in SPI differ from CSR and CPA, as sociopolitical issues are divisive, emotionally charged, and institutionally contested (Nalick et al., 2016). Additionally, objectives regarding sociopolitical activities are usually unknown a priori (Bhagwat et al., 2020). CPA is generally aligned with organisational interests (Lux et al., 2011; Werner, 2017). By contrast, SPI can be diametrically misaligned with regulators or policymakers. However, in both CSR and CPA, a close relationship typically exists between these activities and organisations objectives. SPI differs since it involves firms taking positions on issues that are characterised by a lack of consensus and a weaker link with business activities (Nalick et al., 2016). Second, while CSR is intended to improve operational relationships with most stakeholders, stakeholder responses to sociopolitical issues vary greatly and depend on stakeholders' sociopolitical values (Bhagwat et al., 2020). SPI does not encompass what would typically be recognised as a CPA, because engagement in sociopolitical activities may not offer a salient competitive advantage to the

organisation (Nalick et al., 2016). Third, while CSR is usually considered as socially acceptable by most stakeholders, CPA can have some unethical or discriminatory ramifications (Mantere et al., 2009). CPA is typically 'egocentric rather than altruistic', with benefits accruing only to the organisations that pursue it (Kim, 2008). The beneficiaries of SPI are not always clear and can sometimes even disenfranchise individual consumers and the organisation. Bhagwat et al. (2020) present the key conceptual differences between these three nonmarket strategies under two streams: Publicity and Partisanship (see Figure 2.4).

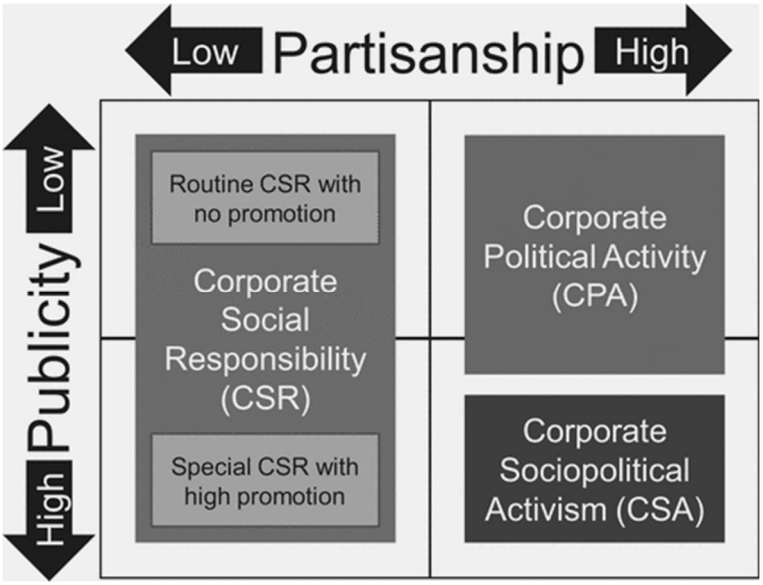


Figure 2.4 Conceptual Distinctions between CSR, CPA and SPI (CSA)

(Source: Bhagwat et al., 2020)

CSR and SPI, for instance, lie on a continuum in terms of their degree of partisanship (Bhagwat et al., 2020). CSR is low in partisanship, because it involves high societal consensus, whereas sociopolitical issues are polarizing. While CSR is intended to improve relationships with most stakeholders (Mishra and Modi, 2016), stakeholder responses to SPI are highly variable and depend on the stakeholders' sociopolitical values (Bhattacharya and Elsbach, 2002). SPI also differs from CSR and CPA in the extent to which each activity is publicised (Bhagwat et al., 2020). While the underlying motivations

to engage in SPI may vary, it is publicly promoted as a communication of an organisation's values (Kotler and Sarkar, 2017; Nalick et al., 2016). By contrast, organisations execute CPA quietly (Lux et al., 2011). For example, Lawton et al. (2013, p. 100) describe lobbying as "a sensitive and often discreet activity that, though publicly available, is often obfuscated".

2.5 Privacy in the Nonmarket Environment

Concepts of privacy as a CSR have been established in the literature for well over a decade. For example, workplace privacy and CSR (SaratChandran, 2005), online privacy concern and CSR (Ashworth and Free, 2006; Pollach, 2011), responsibility and privacy concern (Bandara et al., 2020; Lwin et al. 2007), and corporate duty and privacy concern (Martin, 2020). However, explorations of privacy as a CPA or an SPI have yet to emerge. This is surprising given that an organisation's nonmarket strategy is shaped by social and political issues (van Marrewijk, 2003) and privacy is considered not just a regulatory activity, but a social and political one (Raab, 2020). For example, organisations invest millions in lobbying for or against privacy (VpnMentor, 2019) and privacy decisions have in the past divided consumer attitudes towards organisations (PEW Research Centre, 2016). Therefore this research reflects on, and integrates, concepts in the nonmarket environment such as those in CSR, CPA and SPI to develop an understanding of organisations' strategies and approaches to NMPv. A significant contribution of this research is the conceptualisation of privacy in the nonmarket environment in this way, thus enabling insight into, and a deeper understanding of, the phenomenon.

This section first begins by tracing the evolution of privacy, from privacy in the physical sense, to privacy of information, outlining key definitions of privacy. Privacy in the nonmarket environment is then presented and a set of key NMPv strategies discussed.

2.5.1 Privacy

The historical roots of privacy are difficult to pinpoint, as some assert its foundations in the writings of Greek philosophers throughout the fourth century (Newell, 1995), whilst others assert that privacy dates back to third century Chinese philosophers (Moore, 1984). Unsurprisingly, these early views of privacy related to the individual's physical environment rather than the privacy of digital information. Since the 1960s, however, discussions and research around privacy have been related to the concept of information privacy (Regan et al., 2013). In addition to this, advances in cloud, mobile, social media, and big data analytics have accelerated and amplified the volume, variety, and velocity of data dramatically (Bauman and Lyon, 2013), particularly in the last decade. These advances have also resulted in increased privacy concerns, as they facilitate the collection and sharing of copious volumes of information, which results in increased privacy concern and greater organisational accountability with regards to managing personal information (Regan et al., 2013).

Privacy has been an issue of concern across a number of academic disciplines, and throughout history. Despite this, definitions of privacy are in disarray and fraught with multiple meanings (Waldo et al., 2007). There is considerable lack of consensus as to whether privacy is a condition, a process, or a goal (Margulis, 1977). The absence of a universally accepted definition of privacy is often attributed to the differing views towards privacy as either personal values or individual rights (Smith et al., 2011). However, the one theme consistent across all definitions is the concept of privacy as 'control' (Belanger and Crossler, 2011; Lundgren, 2020; Menges, 2021). Warren and Brandeis (1890) laid the foundation for the concept of privacy known as 'control over information about oneself' (DeCew, 2002), a concept endorsed by more recent classical commentators such as Alan Westin, Irwin Altman, and Stephen Margulis. For example, Westin (1967) defines privacy as the claim of individuals, groups, or institutions to control when, how, and to what extent

information about them is communicated to others. Altman (1975) defines privacy as the mechanisms of control over the concealment of information, and Margulis (1977) defines privacy as the control of transactions between people rather than just information. However, the need for control over privacy is not static and evolves with time and context. Westin (1967) for instance, describes privacy as a dynamic process changing over time, and Altman (1975) posits that the need for privacy is dynamic across both time and situation. These definitions are summarised in Table 2.5.

Table 2.5 Definitions of Privacy as Control

Year	Author	Definition
1890	Warren and Brandeis	Control over information about oneself.
1967	Westin	The claim of individuals, groups, or institutions to control when, how, and to what extent information about them is communicated to others. A dynamic process changing over time.
1975	Altman	Mechanisms of control over the concealment of information, the need for which is dynamic across both time and situation.
1977	Margulis	The control of transactions between people rather than just information.

Our ability to control both information and access to us, allows us to control our relationships with others. Hence privacy is also connected to the control of our human behaviour and activities (Rachels, 1975) and is fundamental for social intimacy (DeCew, 2002). Fried (1970) argues privacy as having intrinsic value fundamental for one's development that enables intimate relationships involving respect, love, friendship, and trust. In his view, privacy is necessary to maintain a variety of social relationships, not just intimate ones (Fried, 1970) and like education, health, and maintaining social relationships, forms an essential part of human flourishing or well-being (Moore, 2003). In summary these descriptions of privacy suggest that varying levels of control are required over privacy about oneself in order to ensure one's own wellbeing, as well as that of society.

Many of these classical definitions of privacy are related to the control of access to information about oneself in a physical sense, rather than a digital sense. During the last few decades however, notions of another form of privacy called 'information privacy' have emerged. Solove (2007) defines information privacy as an umbrella term for a set of privacy problems resulting from information collection, information processing, information dissemination, and privacy-invasion activities. Information privacy, as distinct from physical privacy, is still a relatively new research area, with information privacy research conducted prior to the 1990s categorised as early information privacy research (Conger et al., 2013). Information privacy has been described as an information asset that can be traded by individuals for benefits and used by organisations to generate revenue (Lessig, 2002). Information privacy can be understood as a specific kind of political situation or condition of a social entity, which is affected by the situations and actions of other social entities (Johnson, 2016). Although information privacy has been described as a subset of the overall privacy construct (Bélanger and Crossler, 2011), a comprehensive definition of information privacy is unlikely due to the many different lenses under which privacy is examined (Pavlou, 2011). Dinev (2014) suggests that societal discourse equates privacy and information privacy, and the terms are used interchangeably in the literature, adding to this definitional ambiguity. However, similar to privacy, many of the definitions of information privacy lean on the conceptualisation of 'control' (Bhave et al., 2020) over the terms under which personal information is acquired and used by an organisation (Gerlach et al., 2019).

Greenaway et al. (2015) highlight four distinct approaches to privacy (called privacy orientations) determined by the levels of control and justice signalled in the organisation's privacy policies. These four orientations are categorised as 'privacy minimisers', 'privacy maximisers', 'privacy differentiators' and 'privacy ignorers'. Figure 2.5 presents CIPO's four primary approaches to privacy.

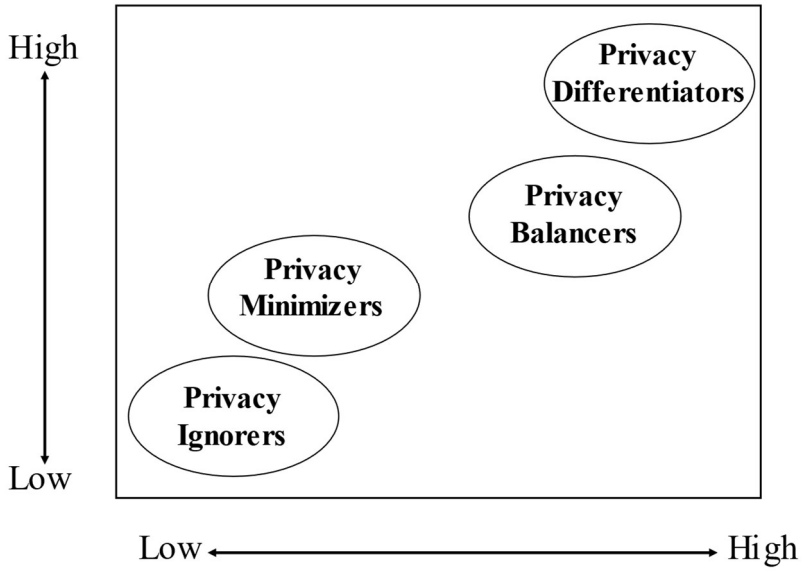


Figure 2.5 Company Information Privacy Orientation

(Source: Greenaway et al., 2015)

CIPO is characterised as "the extent to which a firm delivers consistent, transparent privacy protection to its customers whilst achieving other organisational objectives" (Greenaway et al., 2015). CIPO is intended to help organisations understand their particular privacy posture toward consumers (Greenaway et al., 2015). The formation of an organisation's CIPO is based on how an organisation reconciles its information management, ethical and legal obligations (Greenaway et al., 2015). However, CIPO does not address the social and political obligations of the organisation regarding privacy.

2.5.2 Nonmarket Privacy

Whilst societal concerns regarding privacy evolved into societal concerns regarding information privacy, organisations' strategic responses towards information privacy also evolved beyond being solely a legal compliance requirement, to also being recognised as a market imperative and critical enabler of trust (Cavoukian, 2016). Westin (2003) presents the evolution of these responses over four decades, beginning in the sixties, into three broad categories: political, societal, and legal. Such responses, he suggests, evolved from

events such as wiretapping, nation state surveillance, and media invasions of privacy. The period spanning 1961 to 1979 is described as the first era of contemporary information privacy development (Westin, 2003), during which discretionary frameworks such as FIPPs emerged. These frameworks combined privacy standards with due process, consumer rights, and equality protections (Westin, 2003). In this period, privacy emerged as an explicit social, political, and legal issue (Laufer and Wolfe, 1977; Westin, 2003).

In the second era, spanning 1980 to 1999, fair monitoring ethical codes in the financial and telecommunication industries were introduced, with increased privacy protections for the wider stakeholder community such as employees. In the third era, spanning 2000-2010, Westin (2003) suggests that information privacy became a first-level social and political issue in response to, amongst others, the bombing of the twin towers, the Internet, the cell phone, the human genome project, data mining, and the automation of government public records. Scherer (2018) and Savitz (2013) also suggest privacy as a social and political issue. The evolution continues into a fourth era, spanning 2010 to the present day, during which societal privacy concerns have emerged in response to advancing technologies such as Big Data (Alashoor et al., 2017) and Artificial Intelligence (AI) (Lobera et al., 2020).

In this thesis, where an organisation includes a privacy activity as part of its CSR agenda, the activity is referred to as a Corporate Social Privacy activity. A privacy activity included in an organisation's CPA practices is referred to as a Corporate Political Privacy activity, and a privacy activity shaped as SPI is referred to as a Sociopolitical Privacy activity. Whilst approaches to Corporate Social Privacy, Corporate Political Privacy and Sociopolitical Privacy are not discussed in the literature, a proposed framework of approaches to NMPv activities is presented in Chapter Three. These three key NMPv strategies are discussed in the remainder of this section. First however, based on definitions of nonmarket strategies previously outlined in Table 2.1, definitions of Corporate Social

Privacy, Corporate Political Privacy and Sociopolitical Privacy are presented in Table 2.6, along with examples of each.

Table 2.6 Nonmarket Privacy Strategies - Definitions and Examples

Nonmarket Privacy Strategy Definition	Based on Nonmarket Strategy Definition	Example of Nonmarket Privacy Strategy
Corporate Social Privacy An evolving umbrella term for a variety of concepts and practices which recognise that organisations have a societal responsibility towards privacy beyond legislation and liability.	**CSR** An evolving umbrella term for a variety of concepts and practices which recognise that organisations have a societal responsibility towards privacy beyond legislation and liability (Blowfield and Frynas, 2005).	**Example** An organisation offering the rights of GDPR to all its consumers regardless of whether the consumers are entitled to them. An organisation offering free downloadable open standards for privacy to the public.
Corporate Political Privacy Corporate attempts to shape government policy and regulation regarding privacy.	**CPA** Efforts made by organisations to influence government policy (Getz, 1993; Hillman et al., 2004).	**Example** An organisation lobbying for privacy regulations. An organisation funding a political action committee with a focus on privacy regulation.
Sociopolitical Privacy An organisation's public demonstration of support (i.e., statements or actions) for or against a wide array of partisan sociopolitical issues with no direct performance motivation.	**SPI** An organisation's public demonstration of support (i.e., statements or actions) for or against a wide array of partisan sociopolitical privacy issues with no direct performance motivation (Nalick et al., 2016).	**Example** A CEO making a public value statement on privacy that may or may not be congruent with all stakeholders values. A group of shareholders writing to the CEO to demand an inquiry into privacy risk of a service or product.

Corporate Social Privacy

Societal concerns regarding social issues often shape an organisation's CSR practices (van Marrejick, 2003) and during the last decade, CSR 2.0 emerged (Visser, 2010). CSR 2.0 is a reference to the influence of Web 2.0 on CSR behaviours (Waddock and McIntosh, 2011) and is defined as socially responsible behaviours that generate positive changes in society (Mosca and Cicera, 2017). Scherer (2018) highlights privacy as one of the key social issues for CSR 2.0. These evolving societal concerns, together with organisational CSR practices, have given rise, in part, to privacy activities exceeding an organisation's legal, financial

and ethical responsibilities, such as Privacy-by-Design[2] standards, developing open privacy standards, or collaborating with privacy advocacy groups. Based on definitions of CSR, as previously outlined in Table 2.6, and Section 2.3.2, Corporate Social Privacy is defined as an evolving term for a variety of concepts and practices, which recognise that organisations have a societal responsibility towards privacy beyond legislation and liability. Whilst similar to the concept of Corporate Privacy Responsibilities from Bandara et al. (2020), Corporate Social Privacy differs in that it is shaped as part of an organisation's nonmarket environment activities. In this way, the stakeholder focus of Corporate Social Privacy is broader, reaching beyond the consumer to include policymakers, governments and society. Reflecting the four discrete perspectives of CSR emerging in response to societal concerns, i.e., stakeholder, political, strategic, and shared value, four similar perspectives of Corporate Social Privacy are posited.

The stakeholder Corporate Social Privacy perspective assumes that organisations consider the privacy concerns of multiple constituencies, including employees, suppliers, consumers, local communities etc. In CSR, the inclusion of privacy has also largely focused on consumers' interests. For example, Pollach (2011) found that of the one hundred CSR reports studied, few reported more than consumer privacy compliance. The individual and consumer, however, remain the primary focus of most privacy regulations and directives.

The strategic perspective of Corporate Social Privacy is driven by organisational concerns about generating value from market-based solutions that address privacy in a socially responsible way. Privacy becomes a strategic and competitive factor as the policies governing data collection and processing start to vary across the market, or even between consumers shopping at the same store (Preibusch et al., 2013). Privacy-by-Design

[2] Privacy by Design or PbD, is a framework of seven foundational principles that embed privacy into the design/operation of IT systems, networked infrastructure, and business practices (Cavoukian, 2006).

(Cavoukian, 2006) enables strategic privacy capabilities by ensuring that software and services have privacy 'baked in' early during product development (Cronk, 2018). Thus, Privacy-by-Design can ensure that costs of enhancing privacy later are avoided, breaches are reduced (Cronk, 2018), and the likelihood of gaining competitive advantage is increased (Hasselbalch and Tranberg, 2016). In this perspective, the objective is to gain market advantage by focusing on nonmarket initiatives that align with consumer values (Kuokkanen and Sun, 2020).

The political perspective of Corporate Social Privacy is associated with political concepts such as national surveillance, freedom of speech, protecting journalistic sources, lobbying, voting, and democracy. Political CSR refers to activities beyond traditional CSR programs in that they place firms in quasi-governmental roles where major decisions about public welfare and social provision have to be made (Valente and Crane, 2010). Organisations invest millions lobbying governments in order to favourably shape legislation in the organisation's best interest (DenHond et al., 2014), for example in order to reduce privacy compliance costs or retain data for longer/further use.

The shared value perspective of Corporate Social Privacy integrates responsibilities to, and from, all stakeholders. The central premise behind the shared value perspective is that the competitiveness of an organisation, and wellbeing of the communities around it, are mutually dependent. For instance, this is illustrated in the emergence of privacy activism, where stakeholders hold organisations accountable for their actions in a socially responsible manner by protesting and using ad-blockers, anonymous search engines and encrypted services (Chandler, 2016; Hasselbalch and Tranberg, 2016). Unless organisations differentiate, they face the prospect of profit-diminishing price competition (Preibusch et al., 2013); the conditions under which personal information is collected can be the source of such differentiation (Preibusch et al., 2013).

Corporate Political Privacy

Privacy regulations, such as the California Consumer Privacy Act (CCPA), or the European Union's General Data Protection Regulation (GDPR), are rules enacted by governments that can limit markets and access to data. Organisations typically try to shape these rules using lobbying to make it more favourable for them (Hillman et al., 2004; Lock and Seele, 2018). As outlined in Table 2.6, Corporate Political Privacy is defined as corporate attempts to shape government policy and regulation regarding privacy. As is the case with CPA (see Section 2.3.2), Corporate Political Privacy most often involves lobbying. Organisations can lobby for privacy regulations that support their business, or lobby to block privacy regulations that harm their business. Large technology organisations have aggressively lobbied governments regarding privacy. For example, in 2018 Apple invested $8.9 million in Corporate Political Privacy (VpnMentor, 2019). There have been concerns that CPA, and by association Corporate Political Privacy, is associated with organisations exerting undue control over governments, legislation, and policies and is consequently distrusted and repudiated (Doh et al., 2012; Lawton et al., 2013). For instance, after CCPA was launched, Facebook, Google, IBM, and Microsoft aggressively lobbied officials to start outlining a federal privacy law to overrule the California law, and instead enact a set of privacy rules that would give these organisations more control over how personal information was handled (New York Times, 2018).

Corporate Political Privacy can lack the altruism associated with Corporate Social Privacy. However it can be incorporated where an organisation tries to shape the rules [for privacy] in a way that balances the common good together with the corporate good (Fremeth and Richter, 2011) or in a way that aims to resolve a public issue (Lock and Seele, 2017). Unlike instrumental lobbying, this type of lobbying aligns with definitions of deliberative lobbying and is therefore referred to in this thesis as deliberative Corporate Political Privacy. An example of deliberative Corporate Political Privacy is provided by Cisco, who

in 2019 lobbied for the US government and global citizens to establish privacy as a human right[3].

Sociopolitical Privacy

While Corporate Social Privacy and Corporate Political Privacy strategies aim to enhance an organisation's competitive position or reputation, some organisations have more recently engaged in privacy-specific nonmarket strategies that demonstrate their support for, or opposition to, privacy as a politically charged social issue. Based on definitions of SPI (see Section 2.4.4), Sociopolitical Privacy is defined here as an organisation's public demonstration of support for or against a wide array of partisan sociopolitical privacy issues with no direct performance motivation. Reflecting the three discrete perspectives of Sociopolitical Political Involvement outlined previously in Section 2.4.4, three perspectives of Sociopolitical Privacy are presented, namely Corporate Sociopolitical Privacy, CEO Sociopolitical Privacy, and Shareholder Sociopolitical Privacy. These perspectives are discussed below.

Corporate Sociopolitical Privacy is defined in this dissertation as an organisation's demonstration of support for, or opposition to, one side of a sociopolitical privacy issue. An example of Corporate Sociopolitical Privacy comes from Apple who, in 2015 and 2016, challenged at least 12 orders issued by the FBI compelling Apple to enable the decryption of phones involved in criminal investigations and prosecutions (PEW Research Centre, 2016). Apple noted in their corporate reports at the time that they "refused to add a backdoor into any of our products". In the US, Apple did not garner widespread support for their decision, with 51% of American smartphone users against Apple's decision and only 38% supporting it (PEW Research Centre, 2016).

[3] https://newsroom.cisco.com/press-release-content?articleId=1965781

CEO Sociopolitical Privacy is defined here as a business leader's personal and public expression of a stance on the privacy debate. An example of CEO Sociopolitical Privacy comes from Salesforce, whose Chairman and CEO, Marc Benioff, called for a national privacy law (Salesforce, 2018) despite that this would require significant investment for Salesforce to address this legislation. Over 70% of respondents to a recent survey selected privacy and data protection as one of the top five issues that they expect CEOs to speak out about and express their opinion on (Weber-Shandwick, 2018).

Finally, Shareholder Sociopolitical Privacy is defined here as actions taken by shareholders with the explicit intention of influencing corporations' privacy policies and practices. An example of Shareholder Sociopolitical Privacy comes from Amazon's shareholders, who in 2019 introduced two voting proposals regarding their privacy concerns for a facial recognition system called Rekognition (Irish Times, 2019). One proposal asks Amazon's board of directors to prohibit sales of Rekognition to government agencies unless its board concludes that the technology does not facilitate human rights violations. The other proposal asks Amazon's board to commission an independent report examining the extent to which Rekognition may threaten civil, human, and privacy rights, and the organisation's finances.

2.5.3 Nonmarket Privacy Key Relationships

Pappas (2018, p. 1683) suggests that "as customers develop both trust and privacy beliefs […] these aspects should be studied together to fully comprehend possible combinations between them, capable of explaining their behaviour". Liu et al. (2005) propose a privacy-trust-intention model to understand a consumer's online behaviour. Thus, it is suggested that these three constructs will also be important in helping to understand a consumer's behaviour in the context of NMPv activities. Having established an understanding of key NMPv strategies and associated activities from the literature, the remainder of this section

aims to shape the foundations for responding to the third research question: *RQ3. What influence do levels of control and justice signalled by nonmarket privacy activities, have on privacy concern, consumer trust and purchase intention/continuance intention?*

Before outlining how the literature reflects the relationships between these three constructs, their definitions are discussed.

2.5.3.1 Definitions: Privacy Concern, Consumer Trust and Behaviour Intention

In the existing literature, the majority of studies harness privacy concerns as the proxy to examine privacy (Bélanger and Crossler, 2011; Xu et al., 2012). It seems reasonable to expect that privacy concern will play an important role in NMPv research. Similar to information privacy, the literature offers an array of definitions to describe privacy concerns, many of which centre on individuals as online customers and pertain to fears regarding possible loss of privacy (Xu et al., 2011), or possible uses of data disclosed online (Son and Kim, 2008). Privacy concerns are personal perceptions that will ultimately influence how the individual perceives a situation involving personal information (Malhotra et al., 2004). Consumer privacy concern is common in privacy studies (Smith et al., 2011), and is generally defined as a consumer's concern about possible loss of privacy as a result of information disclosure to an online business (Kim and Huh, 2017; Xu et al., 2008). There are many factors that may create privacy concerns including, unauthorised access, secondary use, and interception of personal information and misuse of such information (Hong and Thong, 2013). Dinev and Hart (2004) summarised those factors and suggested two main antecedents of privacy concerns; perceived potential privacy risk when personal information is revealed, and perceived loss of ability to control the submitted personal information.

Perceptions of privacy risk control not only increase users' privacy concerns, but can potentially create a situation where users distrust organisations and hesitate to disclose personal information (Libaque-Saenz et al., 2016). Hence, it is important that organisations are capable of building trust (Mutimukwe et al., 2020). Trust is well established as the expectation regarding an organisation's future behaviour (Holtz, 2013). The most common definitions of trust centre around the idea that one expects another to act in a particular manner based on their ability and willingness to do so – and is often referred to as competency-based or benevolence-based trust (Sitkin and Roth, 1993). Another type of trust, which receives less attention in the literature, is values-based trust or value-congruence (Tomlinson et al., 2014). This type of trust infers that one parties' values are in congruence with our own, so that unforeseeable situations will be approached by them in a similar way to us (Tomlinson et al., 2014). Rousseau et al. (1998) define trust as the psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behaviour of another. Mayer et al. (1995) define trust as the willingness of a party to be vulnerable to the actions of another party (Mayer et al., 1995). The willingness to be vulnerable is judged based on dimensions of trustworthiness (Mayer et al.,1995). The key dimensions of trustworthiness are ability, benevolence, and integrity (Mayer et al., 1995). Abilities are domain-specific skills and competences that facilitate the development of trust between parties. Benevolence is the extent to which one is perceived to be acting in good faith and wanting good for another, even in the absence of any personal rewards or gains (Mayer et al., 1995; Mesquita, 2007). Integrity is the willingness of the trustee to adhere to principles that a truster subscribes to. In this way, trust reflects a consumer's overall perception of their willingness to depend on an organisation's benevolence, integrity, and competence (Bandara et al., 2020; Akter et al., 2011; Mou et al., 2017).

Trust can be classified into a number of broad categories (Rousseau et al., 1998, McKnight and Chervany, 2002), such as institutional trust (trust in regulatory systems and organisations), generalised trust (trust in others), calculative trust (rational evaluation that others are likely to behave in a way that does not cause harm for their own interests), and relational trust (derived over time based on interactions between the trustor and trustee and could derive from familiarity and experience (Schoder and Haenlein, 2004). Institutional trust refers to an individual's confidence that the data-requesting medium will not misuse his or her data (Dinev and Hart, 2006; Bansal et al., 2010; Anderson and Agarwal, 2011) and has been found to be related to privacy concern (Bansal et al., 2010), risk beliefs (Malhotra et al., 2004), and intention to disclose information (Dinev and Hart, 2006). Institutional trust captures when individuals assess favourable conditions for transactions through norms, procedures, and controlling mechanisms and is specific to a context such as an industry or type of business (Pirson et al., 2017).

Pirson et al. (2017) distinguish between interpersonal trust and organisational trust as it relates to stakeholder perspectives, i.e., interpersonal trust describes the extent to which individuals trust other individuals along relevant trustworthiness dimensions, whereas organisational trust describes the extent to which individuals trusts an organisation. Stakeholder trust is closer to personalised trust, in that an individual is willing to accept vulnerability of the actions of a particular organisation. As such, stakeholder trust is influenced by both the general trusting belief of the consumer (trustor) and the ability, benevolence, and integrity of the organisation (trustee) (Mayer et al., 1995; Pirson et al., 2017). Stakeholder trust in an organisation, then, entails the willingness of individuals (customers, employees, etc.) to accept vulnerability to the actions of an organisation, based on positive expectations (Pirson et al., 2017):

According to Ajzen (1991), intentions are assumed to capture the motivational factors that influence a behaviour, they are indications of how hard people are willing to try or how

much of an effort they are planning to exert, in order to perform the behaviour (Ajzen, 1991, p.181). Behavioural intentions come in many forms, including purchase intention, repurchase intention, continuance intention, recommendation intention, and feedback intention, among others (Gao et al., 2015). Continuance intention is defined as an information system user's intention to continue using an information system (Bhattacherjee, 2001). Purchase intention is defined as a customer's willingness towards purchase actions (Meskaran et al., 2013) or as a situation where a customer is willing, and intends, to conduct online transactions (Pavlou, 2003).

2.5.3.2 Relationships Between Privacy Concern, Trust and Intentions

In the privacy literature, trust has attracted much attention (Hong and Thong, 2013; Malhotra et al., 2004; Waldman, 2018). Strong relationships have been found between privacy and trust (e.g., Bansal et al., 2015; Bansal et al., 2016; Hong and Thong, 2013; Kumar et al., 2018; Malhotra et al., 2004; Pavlou et al., 2007; Tsarenko and Tojib, 2009). Trust has been identified as an important determinant of continuance intention (Lee et al., 2015) and purchase intention (e.g., Hong and Cho, 2011; Hung et al., 2012). Privacy concern has also been identified as a key factor predicting purchase intentions (Belanger et al., 2002). However, there is substantial controversy regarding the relationship between privacy, trust and behaviours (Miltgen and Peyrat-Guillard, 2014), necessitating calls for more research to offer a deeper understanding of the relationship among privacy, trust, and behaviours (Miltgen and Peyrat-Guillard, 2014, p. 106). For instance, trust is found to relate to both privacy and disclosure e.g., Fogel and Nehmad (2009), and to mediate between them e.g., Dinev and Hart (2006). Privacy concern is found to be an antecedent to trust (e.g., Bélanger et al., 2002; Benamati et al., 2017; Eastlick et al., 2006) or a consequence of trust (e.g., Malhotra et al., 2004). Trust may also moderate the relationship (e.g., Bansal et al., 2010), so that privacy concern has a weaker effect on behaviour, relative to trust (e.g., Ba and Pavlou, 2002). Bandara et al. (2020) found that organisations

experience increased consumer trust and reduced privacy concerns when their data practices include ethical privacy responsibilities and not just legislative responsibilities.

In the nonmarket literature, trust also has attracted much attention (e.g., Du et al., 2010; Tsai et al., 2015; Vlachos et al., 2010). Multiple studies have shown that customer perceptions of an organisation who behaves in a socially responsible manner are positively related to trust in the organisation (e.g., Kim, 2019; Martínez and del Bosque, 2013; Swaen and Chumpitaz, 2008). Nonmarket activities that reflect values of justice are associated with signalling dimensions of integrity (Park et al., 2014) and benevolence (Hess, 1995). Values of fairness, typical in CSR strategies, can lead to increased trust (Liedong et al., 2014; DenHond et al., 2014). Trust is considered an outcome of CSR (Chernev and Blair, 2015; DeRoeck and Delobbe, 2012; Homburg et al., 2013) and also considered to be the mediating variable that links nonmarket strategy (CSR) with business benefits such as increased revenues (Du et al., 2007) and positive employee behaviours (Gaudêncio et al., 2017). When a consumer positively perceives an organisations commitment to CSR, it can lead to increased consumer trust (Choi and La, 2013; Castaldo et al., 2009; Martínez and del Bosque, 2013); where a consumer negatively perceives an organisations commitment to CSR, it can lead to reduced consumer trust (Pivato et al., 2008). On the other hand, CPA is undertaken by organisations as a reaction to issues that directly affect only themselves (Hillman and Hitt, 1999) and benevolence is often missing in CPA (Liedong et al., 2014). Distrust, the inverse of trust, has also been associated with CPA due to its potential association with corruption and the fear of organisations exerting undue influence on governments (Doh et al., 2012; Lawton et al., 2013).

In the nonmarket environment, several studies also explore the relationship between nonmarket strategy and purchase intention (e.g., Abdeen et al., 2016; Amoroso and Roman, 2015; Bianchi et al., 2019; Dodd and Supa, 2015; Mulaessa and Wang, 2017). SPI (e.g., the sociopolitical issue of same-sex marriage) was found to be significantly

associated with purchase intention (Dodd and Supa, 2015), and CSR was found to have a direct positive relationship on purchase intention (Zhang and Ahmed, 2021). CSR practices have been found to have a negative relationship with purchase intention where consumers perceive that the practices increase the organisation's cost or reduce the quality of the product (Sen and Bhattacharya, 2001). In contrast, CSR practices, that are considered congruent with consumer values, can lead to increased purchase intention (Martínez and del Bosque, 2013; Park et al., 2017) and increased consumer trust (Iglesias et al., 2020).

2.6 Summary of the Research and Knowledge Gaps

The need for further exploration of privacy in the context of the nonmarket environment, is discussed below for two disparate literatures; the privacy literature and the nonmarket environment literature.

The Privacy Literature

Organisations struggle to balance the need for privacy with the need to monetise data (Bauman and Lyon, 2013) and have traditionally considered privacy as a compliance cost, including costs associated with auditing, regulatory fines, and breach remediation. However, approaching privacy in this way runs the risk of overlooking the benefits of privacy to the organisation beyond compliance requirements, such as increased consumer trust and reputation (Goldberg et al., 2003) and reduced privacy incidents (Accenture and Ponemon Institute, 2015; Culnan and Williams, 2009). Although privacy activities beyond regulation are clearly important, there is little guidance in scholarship to help provide an organisation with a comprehensive understanding of these activities. This research fills this gap by identifying and describing privacy activities associated not only with an

organisation's legal and financial responsibilities, but also with their ethical and societal responsibilities.

The privacy literature can be organised into two broad streams. The first involves consumer-level research such as the measurement of privacy concerns (Sheehan and Hoy, 2000), and the examination of the specific conditions that individuals are willing to provide personal information under (e.g. Phelps et al., 2000). The second stream is concentrated on organisations ethical, legal, regulatory, and corporate responsibilities concerning online privacy (e.g. Ashworth and Free, 2006; Caudill and Murphy, 2000; Pollach, 2011). Analysis in the literature is typically focused at the individual level, i.e., control is most often explored as a consumer requirement that reduces privacy concerns (Pavlou and Fygenson, 2006; Phelps et al., 2000; Xu, 2007). However, control is also relevant from an organisational standpoint, as the notion of control extends beyond strictly individualistic approaches (Lazaro and Le Metayer, 2015). This viewpoint is very much overlooked in the literature. Studies combining the control and justice viewpoints are rare. This is surprising given that consumers' conditions regarding personal information and organisations' conditions for personal information are inextricably linked. This research fills this gap in the context of NMPv, by combining consumer level research with organisational level research.

Ginosar and Ariel (2017) highlight how the study of online privacy addresses three separate domains: user privacy concerns and behaviour, website privacy notices and practices, and national regulations. However, such an approach overlooks organisations' activities in the nonmarket environment, such as their lobbying activity and their CSR reports. Anic et al. (2019) develop an extended model of the relationship between individual and societal determinants of online privacy concern and behavioural intention of internet users. They present an extended model of antecedents to and consequences of privacy concern They highlight for the first time the societal element that influences

privacy concern. In their model, they use individual family values. This research highlights that an individual's values towards privacy also reflect societal expectations, expectations which are changing all the time (Johnson, 2019).

In response to an organisation's privacy practices, consumers can also form intentions, such as purchase intention (Creyer, 1997), continuance intention (Bhattacherjee, 2001), intention to share personal data, or intention to use new technology (Anic at al., 2019). Neither Krishen et al. (2017) nor Lwin et al. (2007) include behavioural intentions as consumer responses in the PRE Model of Privacy. Including intentions is important, as intentions are the most influential predictor of a consumer's actual behaviour (Ajzen, 1991), and are associated as responses to privacy concern (Fortes and Rita, 2016) or responses to consumer trust (e.g., Kim et al., 2009; Kim et al., 2010; Liao et al., 2011).

Bélanger and Crossler (2011, p. 1029) emphasise that privacy researchers should start considering organisations' own demands and requirements with regard to customer information. To date, only two studies have addressed this particular challenge (Greenaway et al., 2015; Greenaway and Chan, 2005). To address this gap, this research presents the privacy activities that are more beneficial to the control needs of the organisation and the privacy activities that are more beneficial to the control needs of the consumer/individual. Greenaway et al. (2015) call for future research to construct a mechanism to measure the amount of control and justice that organisations demonstrate in their approach to protecting privacy. Finding that no such mechanism exists and recognising the value that such a mechanism would bring to privacy researchers and privacy practitioners, this research fills this gap by building such a mechanism.

Organisational trustworthiness has been associated with perceived regulatory effectiveness (Xu et al., 2011) and has been found to improve stakeholder relationships through steps such as investing in CSR, satisfying the needs and interests of constituents, and lobbying

policymakers (Barnett, 2007). Yet in the context of privacy, such trust mechanisms have not been explored in the literature. This research fills this gap by exploring the influence of different NMPv strategies, namely Corporate Social Privacy and Corporate Political Privacy, on consumer trust.

Mutimukwe et al. (2020) use FIPPs and voluntary industry standards, as demonstrated through an organisation's privacy policy, to determine levels of risk-control signalled by the organisation Greenaway et al. (2015) apply FIPPs, as demonstrated through an organisation's privacy policies, to interpret and establish levels of control and/or levels of justice signalled by organisations to their consumers. As previously noted, there are a number of issues with the application of FIPPs in the literature: namely that in the EU, the principles of FIPPs are enshrined within the GDPR. Therefore, in the GDPR context, the principles of FIPPs represent the more legal element of control rather than justice.

The Nonmarket Environment Literature

In 2021, The Journal of Management Studies launched a call for papers for a special issue on corporate social and political strategic objectives. The call highlighted how academic inquiries into CSR and CPA have been slow to develop and a lack of integrated understanding of how firms develop relationships with their social and political stakeholders in nonmarket environments (Lawton et al., 2014; Mellahi et al., 2016; Scherer et al., 2016). This research responds to the call by developing an approach to NMPv that integrates concepts of social and political perspectives of nonmarket strategy.

The linkage between social and environmental nonmarket practices and firm performance has been extensively studied (Wrona and Sinzig, 2018) and largely confirmed (Wiengarten et al., 2012). Whilst privacy has been identified as a social nonmarket environment practice (Savitz, 2013) and as a CSR (Flyverbom et al., 2019; Martin, 2016; Howe and Nissenbaum, 2009), there is still a surprising dearth of research exploring privacy as a CSR

(Scherer, 2018). Similarly, organisations invest heavily in Corporate Political Activities (CPA) aimed at controlling and shaping privacy regulations, yet extant privacy research has not explored the effects of privacy-specific CPA. This research responds to this dearth by adding to the scholarship exploring privacy as CSR and by extending this scholarship with concepts of social and political perspectives of NMPv.

Empirical research has not paid sufficient attention to the joint consideration of CPA and CSR and their consequences for stakeholders (Tortosa-Edo and Lopez-Navarro, 2020). While scholars have long articulated the need for their integration (Baron, 2001; McWilliams et al., 2002; Rodriguez et al., 2006; Siegel, 2009), there has been little exploration of the interactions between nonmarket strategies until more recently (DenHond et al., 2014; Frynas and Stephens, 2015; Hadani and Coombes, 2015). This research jointly considers the influence of Corporate Social Privacy and Corporate Political Privacy on outcomes for the consumer.

Many existing studies do not highlight synergies or tensions of various theories or integrate such perspectives in their empirical research (Mellahi et al., 2016). The result of these failures means that the CPA and CSR literatures do not explain or explore their relationship with privacy when both strategies are clearly involved in privacy and pose both synergies and tensions. This research fills these gaps in the literature by exploring privacy in the context of the nonmarket environment. Because extant literature has predominantly neglected this important aspect of privacy, the overarching aim of this research is to provide a gateway to deeper research into the phenomenon of nonmarket privacy.

Multiple studies have shown that customer perceptions of an organisation/brand who behaves in a socially responsible manner are positively related to trust in the organisation/brand (e.g., Martínez and del Bosque, 2013; Swaen and Chumpitaz, 2008).

However, neither CPA nor CSR studies have empirically dealt with the central issue of individual's trust (Vlachos et al., 2010). This is surprising, as studies have linked privacy and trust (Malhotra et al., 2004; Hong and Thong, 2013), privacy and social responsibility (Pollach, 2011), and trust and social responsibility (Du et al., 2007; Tsai et al., 2015; Vlachos et al., 2010). To address this gap, this research measures the influence that an organisation's NMPv activities has on consumer trust.

The gaps in these two disparate literatures are summarised in Table 2.7.

Table 2.7 Summary of the Gaps in the Literature

Category	Gap	Relevance	Addressed in this research by:
Taxonomy/ Classification	Organisations struggle to balance the need for privacy with the need to monetise data. Privacy is traditionally considered as only a compliance cost.	The risk of overlooking the benefits of privacy to the organisation beyond compliance e.g., increased consumer trust, reduced breaches.	Identifying and describing privacy activities associated with an organisation's legal, financial, ethical, political and societal responsibilities.
Calls for Research	Greenaway et al. (2015) call for future research to construct a mechanism to measure the amount of control and justice that organisations demonstrate in their approach to protecting privacy.	No such mechanism has yet been constructed.	The Nonmarket Privacy Orientation Matrix is constructed.
	2021 call for papers in Journal of Management Studies highlighted the lack of an integrative understanding of how firms develop relationships with their social and political stakeholders in nonmarket environments.	Call for further theory development and empirical inquiries into the research areas of CSR and CPA have not yet emerged for privacy in the context of the nonmarket environment.	Developing an approach to NMPv that integrates concepts of social and political perspectives of nonmarket strategy.
Integration	The literature is typically focused on exploring control at the individual level, overlooking how control is relevant from an organisational standpoint. Calls for privacy researchers to consider organisation's demands and requirements (Belanger and Crossler, 2011).	For personal information, control requirements for the consumer and control requirements for the organisation are inextricably linked.	Combining consumer level and organisational level NMPv research. Determine the NMPv activities that are more beneficial to the control needs of the organisation and the NMPv activities that are more beneficial to the control needs of the consumer/individual.
	While the linkage between social and environmental nonmarket practices and firm performance has been extensively studied, there is still little scholarship in the area of privacy as a nonmarket environment activity.	Whilst the privacy literature does explore privacy as a CSR, it has not explored the effects of privacy-specific CPA, even though organisations invest heavily in CPA aimed at shaping privacy regulations. Literature also does not explore privacy as an SPI even though organisations clearly conduct it.	Adding to the scholarship already exploring privacy as CSR, and extending this by integrating concepts of social and political perspectives of NMPv.
	Whilst much scholarship highlights the need for joint considerations of CPA and CSR, and their consequences for stakeholders, there has been little exploration of them in this way.	Empirical research has not paid sufficient attention to the joint consideration of CPA and CSR and their consequences for stakeholders.	Jointly considering the influence of social and political perspectives of NMPv on outcomes for the consumer.
	Many existing nonmarket environment studies do not highlight synergies or tensions of various nonmarket environment theories or integrate such perspectives in their empirical research.	The CPA and CSR literatures do not explain or explore their relationship with privacy even though both strategies are clearly involved in privacy and pose both synergies and tensions.	Exploring privacy in the context of the nonmarket environment to provide a deeper understanding of NMPv.

Category	Gap	Relevance	Addressed in this research by:
Trust and Privacy	Customer perceptions of an organisation behaving in a socially responsible manner are positively related to trust. However, neither CPA nor CSR studies have empirically dealt with the central issue of individual's trust.	This is surprising as studies have linked privacy and trust, privacy and CSR, and trust and CSR.	Measuring the influence that an organisation's NMPv activities have on trust.
	Organisational trustworthiness has been associated with regulatory effectiveness and improved stakeholder relationships through CSR. However, such trust mechanisms have not been explored in the context of privacy.	CSR, CPA and privacy are all associated with signals of trustworthiness. Therefore NMPv would be expected to similarly be associated with these signals.	Exploring the influence of different NMPv strategies, namely Corporate Social Privacy and Corporate Political Privacy, on consumer trust.
	Neither Krishen et al. (2017) nor Lwin et al. (2007) included behavioural intentions as consumer responses in the PRE Model of Privacy.	Consumers can also form intentions, such as purchase intention (Creyer, 1997), continuance intention (Bhattacherjee, 2001), or intention to share personal data or intention to use new technology (Anic at al., 2019).	Continuance intention and purchase intention are included as consumer responses to NMPv activities.

3 CHAPTER THREE: FRAMEWORKS AND HYPOTHESES

3.1 Chapter Introduction

Taking a mixed methods approach, this research consists of two studies, referred to as Study One and Study Two, with each study serving to address specific research questions previously discussed in Section 1.4. The purpose of this chapter is to present the theoretical research model(s) for Study One and Study Two, and to outline the primary hypotheses examined in Study Two. This chapter builds upon the literature review in Chapter Two, to develop these research model(s) so that the research questions and the gaps in our knowledge regarding privacy in the nonmarket environment, can be addressed.

3.2 An Overview of the Research Phases

Study One is first concerned with addressing RQ1 and RQ2, by constructing a framework of organisational NMPv orientations and their associated NMPv activities, and is grounded in control and justice theory. In Study One, a thematic analysis of 90 CSR reports is undertaken. Study Two is grounded in PRE Theory and is concerned with addressing RQ3. Study Two uses an experimental vignette methodology (EVM) to measure consumers responses to NMPv activities, namely their privacy concern, their trust in the organisation and their purchase intention/continuance intention. The NMPv activities described in Study Two are established in Study One. See Figure 3.1 for a visualisation of both studies and their integration.

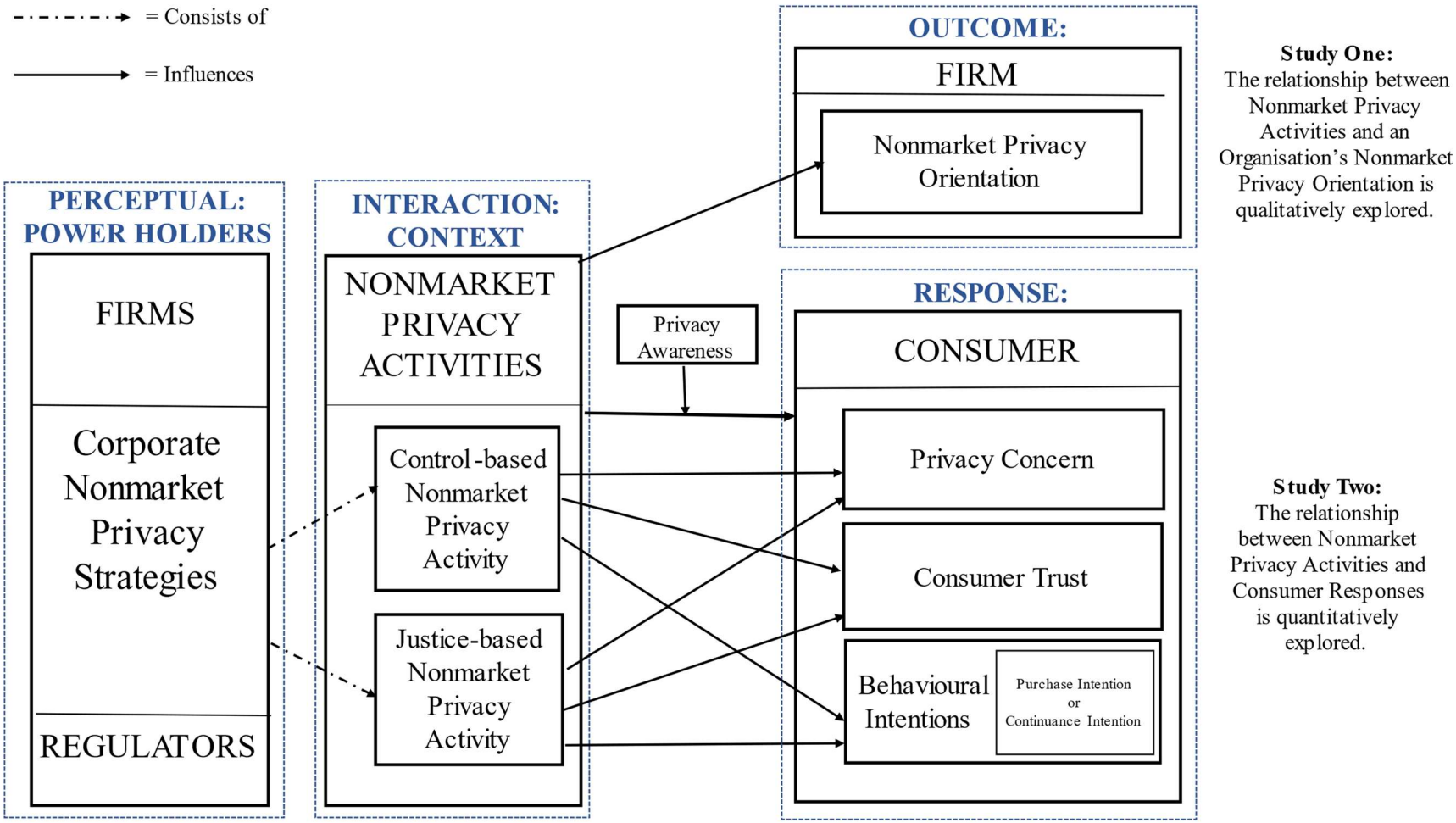


Figure 3.1 Overall Research Approach

The remainder of this chapter outlines the two studies. First, combining control and justice theory, together with theories of CSR, the research model for Study One is described. By reflecting on current approaches to privacy, and integrated approaches to nonmarket strategy, a set of four proposed NMPv orientations (called the Nonmarket Privacy Orientation Matrix) are then described. This theoretical framework explains an organisation's NMPv orientation, as characterised by the levels of control and justice signalled by their reported NMPv activities. Integrating theories of control and justice with PRE theory, the theoretical research model for Study Two is presented. The hypothesised relationships within this model are then outlined and justified, and the dependent variables described. The chapter concludes with a brief summary of the key hypotheses in the research and an outline of the next steps.

3.3 Study One: Proposed Research Framework

This research applies control and justice theory to help determine and explore NMPv approaches, as outlined in Figure 3.2.

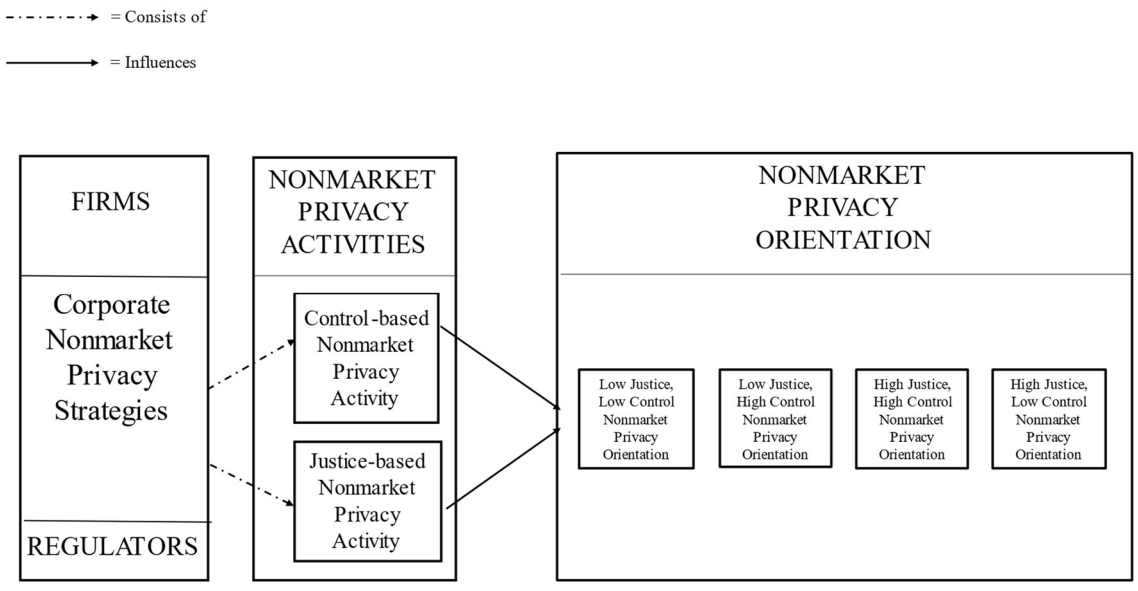


Figure 3.2 Study One Research Model

In the nonmarket environment literature, there have been several attempts to categorise approaches to nonmarket strategies (Castello and Lozano, 2009; Trapp, 2012). Section 2.4.2 presents these approaches as CSR Postures from Castello and Lozano's (2009), and CSR Generations from Trapp (2012). In the privacy literature, approaches to privacy (CIPO) have been described by Greenaway et al. (2015). As described in Section 2.5.1, control and justice theories are applied in combination by Greenaway et al. (2015) to characterise approaches to privacy. Greenaway et al.'s (2015) use of control and justice theory to explore privacy in this way, forms the starting point for the theoretical framework applied in Study One of this research. Similar to CIPO, we follow Greenaway et al.'s (2015) interchangeable use of the terms orientation and approach. Thus, approaches to NMPv are referred to in this research as 'NMPv orientations'. In this research however, the formation of an organisation's NMPv orientation extends beyond the dimensions of CIPO, i.e., information management, ethical and legal obligations, to include reconciling the complex interconnection between an organisation's core activity and the greater global context of privacy. As such, the formation of an organisation's NMPv orientation also includes the organisation's social and political obligations regarding privacy. Reflecting definitions of approaches to CSR from Trapp (2012), an organisation's NMPv orientation is defined here as an organisation's approach to, and understanding of, its legal, social and political responsibilities towards protecting privacy, the NMPv programs it develops to implement privacy protection, and how it frames and communicates its privacy activities.

This research integrates approaches to nonmarket strategy, i.e., CPA and CSR, as suggested by Lawton and Rajwani (2015), and characterising these approaches in terms of control and justice signalled by them, similar to CIPO. The researcher hypothesises the existence of at least three primary NMPv orientations, namely Risk Management, Integrated and Citizenship. The Risk Management NMPv orientation is characterised by low-control and low-justice; the Integrated NMPv orientation is characterised by high-

control and low-justice; and the Citizenship NMPv orientation is characterised by high-control and high-justice. However the researcher posits a fourth orientation, beyond the approaches noted by Castello and Lozano (2009) or Trapp (2012), which is characterised by high justice and low control. In this way the researcher extends CSR postures from Castello and Lozano (2009) with this additional posture referred to as the Warrior Posture. In this hypothesised posture, the Warrior takes a values-based approach to nonmarket activities and will participate in protests, or refuse to be compliant to regulation/court orders, where such requirements have the potential to infringe on societal rights and freedoms. The Warrior posture will even alienate certain stakeholders in order to address social issues such as privacy. Reflecting this extension, the researcher also extends Generations of CSR from Trapp (2012) to include a Fourth Generation of CSR. In this generation, organisations not only spearhead social change, but demonstrate a commitment to certain social values to the extent they will challenge legislation or refuse to be compliant to it, if they feel that such compliance would infringe on societal rights and freedoms.

Table 3.1 presents an overview of the theoretical formation of NMPv orientations, generations and perspectives proposed in this research, including the hypothesised approaches to NMPv activities and hypothesised extensions to current approaches to CSR i.e., CSR Postures and CSR Generations.

Table 3.1 Nonmarket Privacy Orientations *(Shaded/Italics = Proposed in this Research*)

	First Generation	**Second Generation**	**Third Generation**	***Proposed Fourth Generation (Extended)***
CSR Generations (Trapp, 2012)	Organisations simply refrain from illegal behaviours.	Organisations secure rights for employees, families, and local communities.	CSR is driven beyond legal and stakeholder to understanding global context. Private, public and social sectors become interdependent. Organisations acknowledge new responsibilities towards society.	*CSR driven by deeply felt values of stakeholders and communities they serve. Can include breaching laws in order to demonstrate commitment to values.*
	Risk Management	**Integrated**	**Citizenship**	***Proposed Warrior Posture (Extended)***
CSR Postures (Castello and Lozano, 2009)	• CSR programs undeveloped. • CSR considered a tool to protect reputation. • CSR related policies and activities focus on highest risk. • CSR compliance focused. • Governance assigned to functional managers. • Strategy/mission not related to CSR agenda. • One-way stakeholder communications.	• Change business models to include social responsibilities. • CSR reports company values towards societal expectations. • Reflects how social issues gain competitive advantage. • Aim to mitigate economic loss medium-term, achieve longer-term gains by responsible practices. • CSR activities are proactive, often using standards e.g., ISO 26000 or GRI. • Top management assigned to CSR programs, strong internal leadership. • Strategic rhetoric reflects CSR. • Stakeholder communications becomes dialogue/collaboration.	• Generate commitment from stakeholders, incorporate social issues as strongly held values. • Associate CSR with other strong values e.g., trust and integrity. • Assuming citizenship role leading social issues. • Broaden agenda by expanding social concerns. • Deepen involvement of top management in leadership of social change. • Form long-term strategic. partnerships with stakeholders to drive social change.	• *Social values held high by top management.* • *Focussed on creating shared value.* • *Implicit social contract exists between stakeholders– a trust that they share values equally, beyond profit.* • *"Warrior role" – top management believe that social values will not be compromised and will breach laws in order to protect those values.* • *Governance structure implemented to ensure values are maintained throughout business.*
NMPv Generations	*First Generation*	*Second Generation*	*Third Generation*	*Fourth Generation*
NMPv Orientations	*Risk Management (Low-Control Low-Justice)*	*Integrated (High-Control Low-Justice)*	*Citizenship (High-Justice High-Control)*	*Warrior High-Justice Low-Control*
NMPv Perspectives	*Compliance*	*Stakeholder, Strategic*	*Stakeholder, Strategic, Shared Value, Political*	*Stakeholder, Strategic, Shared Value, Political*

Similar to the orientations described in CIPO (Greenaway et al., 2015), an organisation's NMPv orientation is best characterised by the levels of control and justice signalled by an organisation's NMPv activities. However, NMPv orientations differ in three key ways from those of CIPO. First, CIPO is described as a 'for-profit' approach to protecting and processing its consumers personally identifiable information (PII), whereas an NMPv orientation is agnostic to organisation type and stakeholders, considering the privacy requirements and concerns of a broader audience.

Second, CIPO reflects the extent to which an organisation's privacy policies affect their customers' abilities to exercise control and justice mechanisms over the processing of their personal information. Rather than focusing on the effect of organisational activities on customers alone, an NMPv orientation seeks to focus on the multiple relationships between the organisation's requirements, the individual's rights, and society's evolving expectations, and reflects the extent to which activities, associated with an organisation's NMPv orientation, signal levels of control and justice. Including these additional privacy activities beyond the market environment is important as the nonmarket environment also contributes to an organisations' bottom line and reputation (DenHond et al., 2014).

Third, CIPO is determined by the level of control and justice demonstrated in an organisation's legal, financial and ethical behaviours, as demonstrated by FIPPs in their privacy policies (Greenaway et al., 2015). There are issues however with the application of FIPPs in this way. FIPPs are applicable in the US, and are discretionary codes; thus, they represent fairness/justice. However, the principles of FIPPs are enshrined in the EU's GDPR as data protection rights and therefore instead represent the more legal element of control (through governance). According to Bandara et al. (2020) most studies focus on consumer perceptions of the privacy policy to conceptualise or measure how corporations exercise power and responsibility (e.g., Lwin et al., 2007; Wu et al., 2012). However, privacy policies often contain little more than terms and conditions (Storey et al., 2009),

and since 2018, the GDPR legislatively prescribes the content of privacy policies in detail (Article 13) therefore standardising and streamlining their content. Therefore, an NMPv orientation is instead determined by the level of control and justice signalled by an organisation's NMPv activities, as reported in their CSR reports. CSR reports are considered legitimate and auditable documents, that are often used to make stakeholders aware of the social and environmental activities and strategies conducted by organisations (Kolk, 2003).

3.3.1 The Proposed Nonmarket Privacy Orientation Matrix

By combining control and justice theory, together with theories of the nonmarket environment, a theoretical framework is constructed that describes and explains an organisation's NMPv orientation, characterised by the levels of control and justice signalled by their NMPv activities. The four NMPv orientations argued by the researcher form the Nonmarket Privacy Orientation Matrix, and is visually presented in Figure 3.3. A description of each NMPv orientation in the matrix follows.

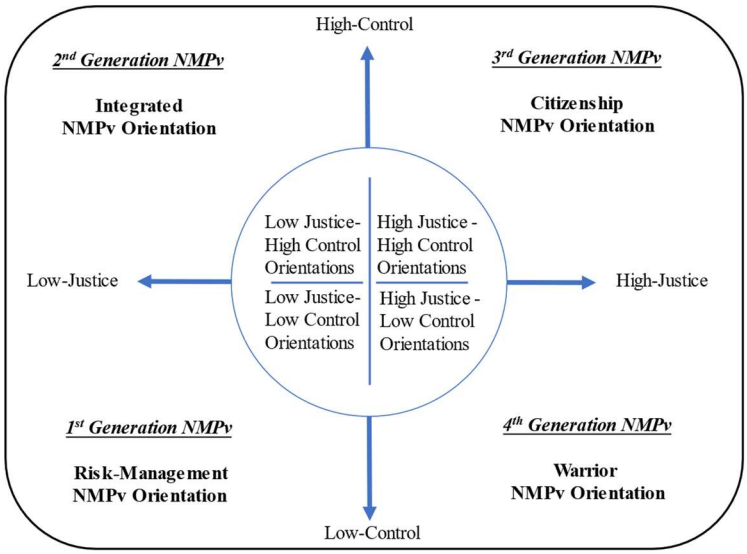


Figure 3.3 The Nonmarket Privacy Orientations Matrix

Risk Management (Low-Justice Low-Control)

The Risk Management NMPv orientation is consistent with the Risk Management CSR posture (Castello and Lozano, 2009), and the first CSR Generation (Trapp, 2012). This NMPv orientation sets compliance as the goal, with governance assigned to functional management. Typically, neither the organisation's strategic positioning, nor the vision or mission, are related to their NMPv activities. NMPv programs can be undeveloped, where NMPv related policies and activities focus on the highest risk privacy activities. NMPv policies and practices are often centred on compliance. Lobbying for privacy may be undertaken, but only where beneficial to the organisation. These organisations offer minimal compliance as part of their nonmarket strategies and agenda.

Integrated (Low-Justice High-Control)

The Integrated NMPv Orientation is consistent with the second CSR Generation (Trapp, 2012) and the Integrated CSR posture (Castello and Lozano, 2009). This NMPv orientation offers robust compliance to regulation. Castello and Lozano (2009) suggest that relinquishing control would not be important to organisations in this orientation, as they focus on maximising profit or efficiency. However, organisations in this orientation will start considering, and respond to, society's evolving expectations (Castello and Lozano, 2009) towards privacy. Johnson (2019) argues that societal expectations towards privacy have been shifting, largely due to the pervasiveness and intrusiveness of the connected world in our daily lives, such as the Internet of Things (IoT). Organisations in this NMPv orientation first extends to the stakeholder perspectives of NMPv, by including privacy rights for employees, their families, and local communities. Relationships with stakeholders will evolve from one-way communication to dialogue and collaboration. Their NMPv orientation also extends to the strategic perspective (Munilla and Miles, 2005), where the organisation actively reflects on ways to use social issues such as privacy

to gain competitive advantage. The objective is to mitigate the erosion of economic value in the medium term and to achieve longer-term gains by integrating responsible privacy practices into daily operations (Zadek, 2004). Top management are assigned the responsibility of managing the NMPv programs across the most important processes in the value chain. NMPv management is proactive and systematic, for example, by using reporting standards such as the Global Reporting Initiative (GRI). The GRI is an international independent standards organisation that helps organisations communicate their impacts on environment and society, such as governance, human rights, social impacts, corruption and climate issues (Global Reporting Initiative, 2021).

Citizenship (High-Justice High-Control)

The Citizenship NMPv Orientation is consistent with the Citizenship CSR posture (Castello and Lozano, 2009) and the third CSR Generation (Trapp, 2012). In the third CSR Generation, organisations openly acknowledge their new roles and responsibilities towards society, and responsibilities towards private, public, and social sectors become interdependent (Latapi-Agudelo et al., 2019; Trapp, 2012). This orientation addresses privacy strategically, where privacy programs are focused on building sustainable relationships, and often exceed regulations. They undertake the CSR perspectives of the previous orientations; however they also undertake political and shared value NMPv perspectives. These organisations not only report privacy metrics, but they reach out to stakeholders, and incorporate privacy as a strongly held value, along with values such as trust and integrity (Mirvis and Googins, 2006). Organisations form long-term alliances with stakeholders to drive change in privacy issues. They deepen the involvement of top management in privacy ‘stewardship’ rather than simple leadership (Caldwell et al., 2010).

Warrior (High-Justice Low-Control)

Similar to the Citizenship NMPv orientation, this orientation positions high on NMPv activities associated with justice. However, unlike the Citizenship NMPv orientation, it is positioned in low control. The Warrior NMPv orientation highlights what they believe is wrong with privacy in society and then act to try to fix it. Compliance is not an absolute in this orientation and can be negotiated if it benefits those social or political beliefs towards privacy. Organisations in the Warrior NMPv orientation may for instance lobby governments for changes to privacy legislation even if they know it will reduce profits/shareholder returns and/or marginalise certain stakeholders. They may stake claims to a particular social value such as privacy, to such a degree that they will not comply with regulations or court orders, if they feel that it would compromise social or democratic freedoms.

3.3.2 Summary of the Theoretical Framework for Study One

The Nonmarket Privacy Orientations Matrix explains an organisation's NMPv orientation and the influence that levels of control and justice have on that orientation. The matrix is applied in Study One to position an organisation's NMPv orientation in one of four hypothesised NMPv orientations, based on the levels of control and justice demonstrated by the organisation's NMPv activities. The matrix is founded in previous scholarship describing approaches to the nonmarket environment, namely CSR Postures from Castello and Lozano (2009) and CSR Generations from Trapp (2012). The Nonmarket Privacy Orientations Matrix is characterised by control and justice theories, similar to CIPO from Greenaway et al. (2015). In developing this framework, the researcher hypothesises four NMPv orientations. The researcher also posits an extension to CSR postures, with the addition of the Warrior posture. Also posited is an extension to CSR Generations, with the addition of the Fourth Generation of CSR. The researcher suggests that neither Trapp

(2012) nor Castello and Lozano (2009) included the Fourth Generation or Warrior posture in their approaches to the nonmarket environment, as the Warrior approach has evolved over the last decade in response to changing societal expectations. Johnson (2019) attributes these societal changes to the pervasive intrusions associated with the connected world. In this way, this research highlights the importance of the role of societal expectations in shaping an organisation's approach to its nonmarket activities, including privacy.

3.4 Study Two: Proposed Theoretical Research Model

Study Two aims to empirically establish the influence that NMPv activities have on constructs considered important to both privacy and the nonmarket, namely privacy concern, consumer trust and purchase intention/continuance intention. Study Two applies a power-based approach to NMPv research. Power is a relational concept that refers to the asymmetric control over valued resources, which in turn affords an entity the ability to control others outcomes, experiences, or behaviours (Tost, 2015). In this way, power can be considered a concept that refers to control over privacy (a 'valued resource'), which in turn affords an entity (the organisation) the ability to control the outcomes, experiences, or behaviours of another (the consumer).

A power-based approach was considered the most appropriate for three reasons. First, power-based approaches to research are theoretically aligned to control-based approaches, as power is often defined as 'control' (Anderson and Brion, 2014; Laczniak and Murphy, 1993). PRE theory (Davis et al.,1980; Laczniak and Murphy, 1993; Murphy et al., 2005, 2005) was selected to explore RQ3, as it has been used previously in both nonmarket scholarship (Liedong et al., 2014) and privacy scholarship (Bandara et al., 2020; Krishen et al., 2017; Lwin et al., 2007) to explore the relationship between power and responsibility

and consumer responses. Second, power has been acknowledged in nonmarket environment scholarship as having critical importance in both CSR (e.g., Banerjee, 2008; Bondy, 2008) and CPA (Frynas et al., 2017). Finally, a power-based approach to research has been identified as a useful ethical and social responsibility approach to investigate consumer privacy issues (Krishen et al., 2017; Martin and Murphy, 2017) and to investigate nonmarket strategies (Frynas et al., 2017). This research thus extends the application of PRE theory to the context of NMPv activities, for the first time.

As discussed in Section 2.5.3, PRE theory states that power should be in equilibrium, where the more powerful partner in a relationship has the societal obligation to ensure an environment of trust and confidence (Lwin et al., 2007). The PRE Model of Privacy (Lwin et al., 2007) holds that consumers who perceive that organisations are acting responsibly in terms of their privacy practices show less privacy concern (Lwin et al., 2007), where consumers react negatively to power imbalances where organisation fail to promote justice in consumer information exchange. In this way, the responsibility demonstrated by powerholders can act as a predictor of potentially damaging customer responses, namely fabricating, withholding or protecting (Lwin et al., 2007). Krishen et al. (2017) extend consumer responses in the PRE Model of Privacy to include personal beliefs and attitudes, e.g., perceptions of fairness, and attitudes towards organisational communications. Bandara et al. (2020) extend the interaction context of the PRE Model of Privacy to include privacy empowerment. Privacy empowerment is commensurate with an individual having control over their information (Bandara et al., 2020), i.e., "a psychological construct related to the individual's perception of the extent to which they can control the distribution and use of their personally identifying information" (van Dyke et al., 2007, p. 71). This would suggest that Krishen et al. (2017) incorporate the consumer's perceptions of justice into the PRE Model of Privacy, and Bandara et al. (2020) incorporate the consumer's perceptions of control.

3.4.1 Key Consumer Responses to Nonmarket Privacy Activities

Krishen et al. (2017) note that there are three key dimensions in the PRE Model of Privacy, namely power holders, the interaction context, and the users' responses. These pillars form the foundations for the theoretical research model used in Study Two. However, the PRE Model of Privacy presents a number of challenges. First, there is an assumption in the PRE Model of Privacy that a direct exchange is taking place between the organisation and the consumer. However not all interactions between a consumer and organisation are direct in this way. For example, a consumer may have purchased a subscription to use an email system, in which case, rather than fabricate/ protect/ withhold, they may discontinue use, or they may move to another system. Consumers can also form intentions, such as purchase intention (Creyer, 1997), continuance intention (Bhattacherjee, 2001), or intention to share personal data or intention to use new technology (Anic at al., 2019).

The second challenge associated with the PRE Model of Privacy is that it assumes an exchange directly affects the consumer, and that they will take actions as a result of that exchange. However NMPv activities can engender a collective, rather than a direct, individual concern. For example, where an organisation's CEO argues against a proposed privacy law, a consumer may not be directly affected, but may still experience privacy concern. Finally, the PRE Model of Privacy assumes that the consumer is privacy aware. However, a number of studies would challenge such an assumption. For example, in 2019, a poll from Proton Technologies (2019), found more than 35% of consumers did not understand their privacy rights or organisations' privacy obligations. Varkonyi et al. (2019) found that whilst 61% of respondents knew what GDPR was, 39% had never heard about it, and only 47% were aware of what GDPR stands for.

To address these challenges, the researcher suggests extending the PRE Model of Privacy to include not only direct consumer responses and cognitive responses, but also consumer intentions e.g., intentions to share personal information, to purchase, to continue use, or to

use new technology etc. The researcher also posits extending the PRE Model of Privacy to include privacy awareness as a moderator of the relationship between the power holders and consumer responses. Thus, in Study Two, the research model includes consumer's purchase intention/continuance intention, and consumer's privacy awareness levels. The three key dimensions of power holders, interaction and consumer responses, associated with the research model in Study Two, are discussed in the remainder of this section.

Powerholders

Lwin et al. (2007) note that two relevant power holders exist: the business policy of the organisation, and the legal/regulatory policy makers. In the research model for Study Two, the organisation and its NMPv strategy are the power holders, in addition to the regulators, and the less powerful partners in the model are the consumers.

The Interaction

In previous scholarship, power has been interpreted as control (e.g., Anderson and Brion, 2014; Laczniak and Murphy, 1993) and responsibility has been interpreted as justice (for example, Fia and Secconi, 2019). Organisations can overstep acceptable levels of control by not demonstrating socially responsible NMPv activity or by undertaking NMPv activities in a way that benefits the organisation and disenfranchises the individual consumer, for example, by lobbying government for reduced privacy rights for consumers. In the Nonmarket Privacy Activities Codebook, control is associated with NMPv activities that express power and influence over data, e.g., corporate political privacy activities. Whereas justice is associated with NMPv activities that express responsibility, e.g., Corporate Social Privacy activities.. In Study Two, NMPv activities demonstrating control or justice represent the context of the Interaction pillar.

Consumer Responses

The factors selected as consumer responses in Study Two, are those considered common to privacy (i.e. privacy concern) and the nonmarket environment (i.e. trust and purchase intention/continuance intention). These constructs are also important from a control and justice perspective, as violations of justice can lead to privacy concern (Culnan and Bies, 2003) together with trust issues and behavioural consequences (Bansal and Zahedi, 2015), and control can lead to privacy concern and negative consumer responses (Benamati et al., 2017; Lwin et al., 2007). Although relationships between privacy concern, trust and purchase intention/continuance intention are already addressed in depth in the privacy literature, including them in the research model for Study Two, offers an opportunity to develop a more holistic nomological network of privacy in the context of the nonmarket environment. Privacy awareness is found to have a strong relationship with both trust and privacy concerns (Benamati et al., 2017; Malik et al., 2016; Warner and Wang, 2019) and therefore privacy awareness is also included. The rationale for the selection of these constructs is discussed in the remainder of this section.

Privacy concern is included in the research model because of its frequent association with control (Pavlou and Fygenson, 2006; Phelps et al., 2000; Xu, 2007) and justice (Culnan and Bies, 2003) and the majority of studies leverage privacy concerns as a proxy to measure privacy (Smith et al., 2011). Consumer trust is included for three reasons. First, both privacy and the nonmarket environment have significant relationships with trust (Donaldson and Preston, 1995; Freeman et al., 2004; Mitchell et al., 1997) and trust has significant relationships with social responsibility (Park et al., 2014; Tsai et al., 2015; Vlachos et al., 2010). Second, several studies have linked privacy and trust (Bansal and Zahedi, 2015; Hong and Thong, 2013; Malhotra et al., 2004). Third, the PRE Model of Privacy (Lwin et al., 2007) was recently extended by Bandara et al., (2020) to include consumer trust. The focus of this research is consumer trust, which is influenced by both

the general trusting belief of the consumer (trustor) and the ability, benevolence, and integrity of the organisation (trustee) (Mayer et al., 1995; Pirson and Malhotra, 2011; Pirson et al., 2017).

As previously noted, both purchase intention/continuance intention and privacy awareness are included. Behavioural intentions (to accept/purchase or continue use) are most often associated as responses to privacy concern (Fortes and Rita, 2016; Thakur and Srivastava, 2014) and responses to trust (e.g., Arpaci, 2016; Kim et al., 2009, Kim et al., 2010, Liao et al., 2011). For instance, Arpaci (2016) found that perceived privacy predicted trust, and consequently, intentions to use mobile cloud storage services. Purchase intention is often considered an outcome of CSR (Mohr and Webb, 2005), and studies have found a relationship between consumer's willingness to purchase services or products, and an organisation's nonmarket strategies (Grimmer and Bingham, 2013). Privacy awareness is included in the theoretical research model for Study Two as previously noted, because previous studies have found that high levels of privacy awareness are associated with higher privacy concern (Benamati et al., 2017), and a consumer's understanding of privacy regulation will significantly influence their privacy concern (Warner and Wang, 2019).

3.4.2 Modelling Consumer Responses

This section first discusses how the literature models the relationships between an organisation's privacy activities and consumer's privacy concern, their trust and their purchase intention/continuance intention, and then discusses how these responses are modelled in Study Two.

As discussed in Section 2.5.3, the literature presents a complex view of privacy concern, where it can play both causal and consequential roles in privacy. Wirtz and Lwin (2009) model privacy concerns as a mediating variable between justice and consumer responses. In the PRE Model of Privacy (Lwin et al., 2007), privacy concern is modelled as a

mediating variable between policy/regulation, and response behaviours. However privacy concerns have also been found not to have an overall effect on consumer responses, and scholars suggest a moderation role for privacy concerns that could interact with trust to determine consumer intentions (Mothersbaugh et al., 2012).

As outlined in Section 2.5.3, the exact role of trust in privacy is unclear because the relationship between these constructs has not been modelled consistently in the literature (Smith et al., 2011). For instance, privacy has been modelled as an antecedent of trust (for example, Liu et al., 2005; Taylor et al., 2009; VanDyke et al., 2007) and trust has been modelled as an antecedent, outcome, and mediator of privacy concern, where often the direction of the relationship between privacy and trust is unclear (Chellappa and Sin, 2005). While some authors have conceptualised trust as an antecedent (Wakefield, 2013) or as an outcome of privacy concern (Bansal et al., 2010), others have argued that trust and privacy concerns are independent factors that may exert separate influences on intentions to disclose information (Dinev and Hart, 2006; Anderson and Agarwal, 2011). Trust has also been modelled as a mediating variable between justice and consumer responses (Wirtz and Lwin, 2009). These complexities have led to ambiguity regarding the relationship between privacy concern and trust across all contexts (Li, 2011). In the context of NMPv activities, this research seeks to determine if there is a relationship between control and justice NMPv activities and consumer trust in the organisation, and not the role that trust plays in the relationship between control/justice and privacy concerns, or control/justice and consumer intentions.

Both trust and privacy concern have been modelled in previous studies as key antecedents to online consumer behaviour (Hoffman et al., 1999). For example, privacy concern has been found to reduce an individual's intentions to use a system and increase intentions to protect, withhold or falsify data (Bandara et al., 2020, Krishen et al., 2017; Lwin et al., 2007). Similarly, trust has been associated with online consumer behaviour (Hoffman et

al., 1999) and consumer responses (Wirtz and Lwin, 2009). However these studies were not conducted in the context of the nonmarket environment. In the nonmarket environment, purchase intention is considered an outcome of nonmarket strategies (Mohr and Webb, 2005), and CSR activities predict purchase intentions (Lee et al., 2009; Murray and Vogel, 1997). Therefore it seems likely that nonmarket privacy activities and consumer trust would similarly influence purchase intentions.

In Study Two, privacy concern, consumer trust, and purchase intention/continuance intention, are modelled as dependent variables. They are modelled in this way for two reasons. First, whilst trust, privacy and resulting consumer responses are closely linked concepts that are usually examined simultaneously (i.e., privacy concern – trust - behaviour intentions), their exact relationship remains a topic of debate (Miltgen and Peyrat-Guillard, 2014). Second, the aim of this research is to explore the influence of control and justice on these constructs rather than determining the whole range of interactions, antecedents, predictors, moderators, mediators etc. Study Two is experimental, where the objective is on isolating causality, rather than testing mediation. Were mediating constructs to be modelled, it would lessen the effectiveness of the experiment as there is a possibility of reverse causality. Figure 3.4 shows how consumer responses to NMPv activities are modelled in Study Two.

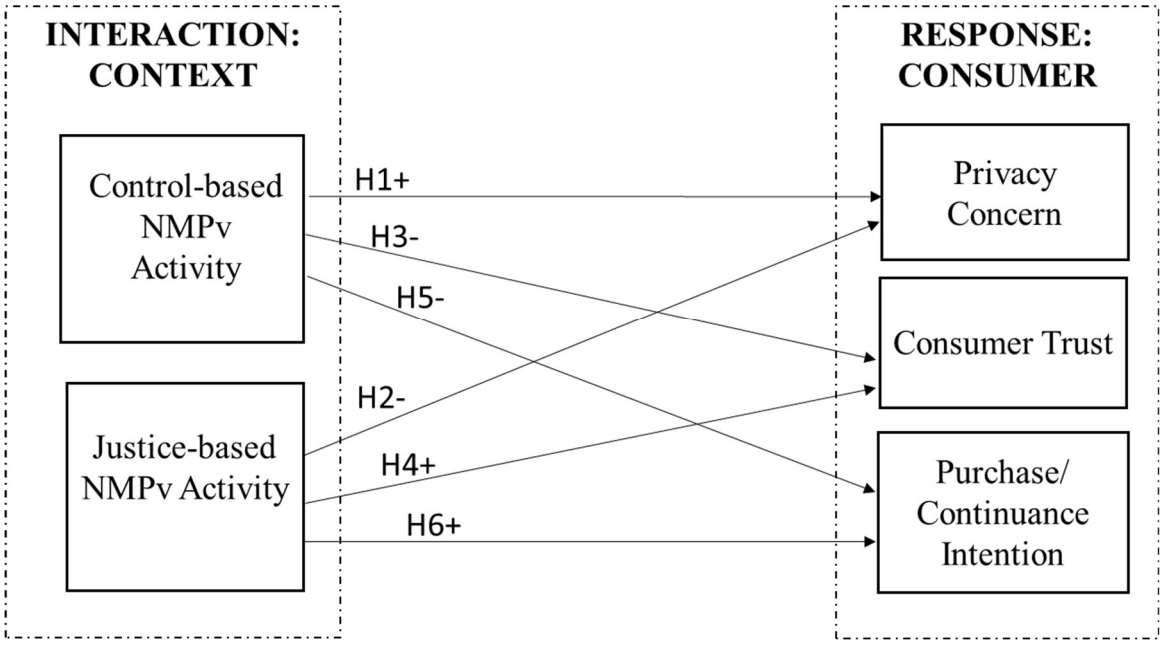


Figure 3.4 Study Two: Modelling of Consumer Responses to Nonmarket Privacy Activities

3.5 Study Two: Hypotheses

In the market environment, an organisation's privacy activities have been found to influence privacy concerns (Smith et al., 2011), trust (Lauer and Deng, 2007; Liu et al., 2005; Wu et al. 2012) and purchase intentions (Hui et al., 2007; Meinert et al., 2006; Peterson et al., 2007). The hypotheses in this section are shaped on the understanding that similar effects from an organisation's NMPv activities would result. Organisations use their activities in the nonmarket environment to control market uncertainty (Parnell, 2019) which can inadvertently create uncertainty in the consumer, resulting in negative consumer responses (Parnell, 2019). An organisation who undertakes nonmarket environment activities that balance the organisation's need for control with the consumers need for control, will benefit in the long run (Caudill and Murphy, 2000) from positive consumer responses. In this way, an organisation's NMPv activities that are intended to control uncertainty in the market, can inadvertently reduce control for the consumer and result in negative consumer responses.

The following section first establishes the context for a set of relevant NMPv activities to include in the experiments, and then presents the hypotheses associated with those experiments.

3.5.1 Establishing Context for a Set of Relevant Nonmarket Privacy Activities

In nonmarket environment research, Frynas *et al.* (2017) found that power is generated through persuasive actions that create legitimacy for corporate policies and practices in the eyes of others. Lobbying is one of these persuasive actions creating legitimacy. Through lobbying, organisations can influence power over the market environment and potentially reinforce this influence through political engagement (Grant, 2000). However, too much power may also result in negative responses from consumers (Lwin et al., 2007), for example, where an organisation's lobbying activity unfairly disenfranchises the consumer. This research proposes that the most likely 'persuasive activity' in an organisation's nonmarket privacy activities that would create an imbalance in power, is the lobbying of government for privacy so that the organisation benefits more than the consumer. This is because such activities can position the organisation with greater power over consumer's data and most likely not be perceived as responsible (Zuboff, 2019). Notably for the consumer, lobbying may also engender concerns about possible loss of privacy for society in general, rather than privacy loss regarding only themselves. Therefore, an organisation lobbying for or against privacy legislation is a foundational component for the context of the experiments.

3.5.2 Hypotheses

The context of the experiment is an organisation's lobbying for, or against, privacy legislation intended to provide governments with access to email systems of all consumers, where the emails will most likely contain personal information such as emails to friends

and family, and sensitive information such as health information, financial information etc. Such a context can be shaped as high-control, where such lobbying benefits the organisation more than the consumer, or it can be shaped as high-justice, where such lobbying benefits the consumer more than the organisation. Applying PRE Theory to this context, the hypotheses in Study Two are visually presented in Figure 3.5. The key hypotheses relate to the relationships between the independent and dependent variables. These relationships are discussed, and the hypotheses presented in the remainder of this section.

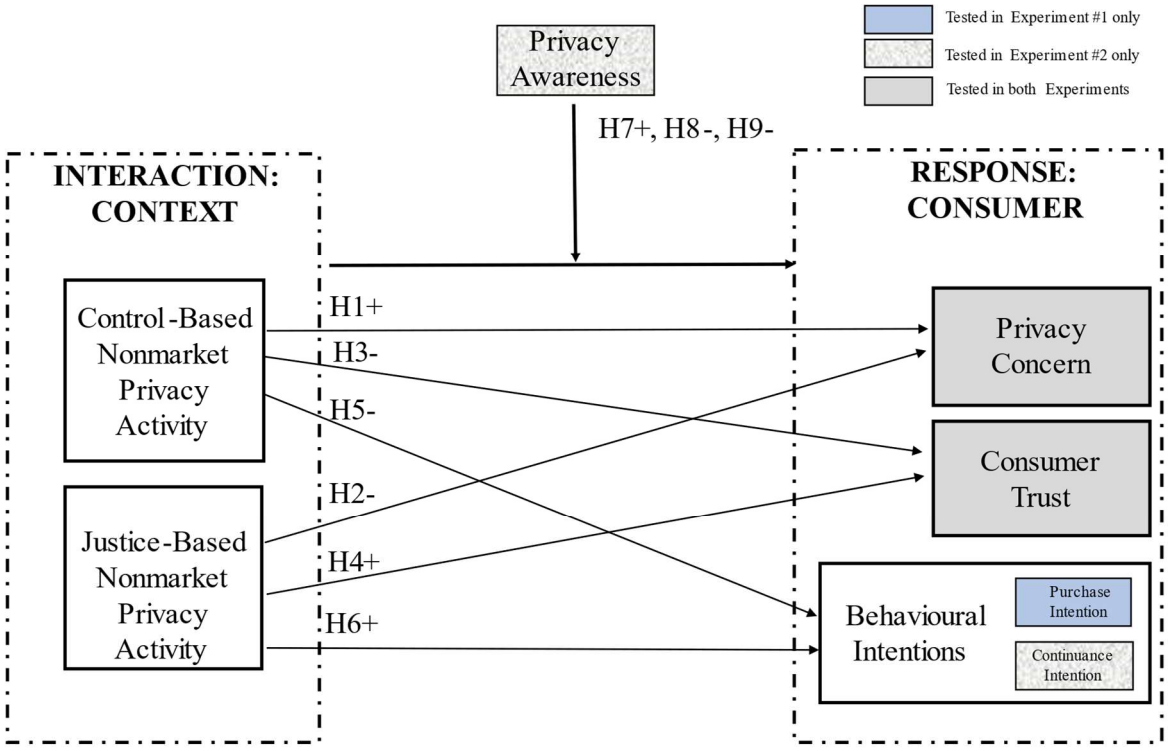


Figure 3.5 Study Two Research Model

3.5.2.1 Nonmarket Privacy Activities and Privacy Concern

Greenaway et al. (2015) posit that levels of control and justice affect privacy concern in the market environment. Levels of control and justice signalled by NMPv activities are expected to similarly influence privacy concern in the nonmarket environment. Both Culnan and Armstrong (1999) and Culnan and Bies (2003) suggest that control is

associated with higher levels of privacy concern. Milne (2000) suggests that consumer privacy concerns are highest when a consumer's perception of control is low. This is supported by empirical studies that find control is critical to the level of privacy concern experienced by consumers (Sheehan and Hoy, 2000), where privacy concern decreases as consumer control over information increases. Justice is also associated with lower levels of privacy concerns (Greenaway et al., 2015; Sheehan and Hoy, 2000).

In the nonmarket environment, where an organisation is seen to have consumer-friendly nonmarket practices, they are perceived as just (Caudill and Murphy, 2000; Liedong et al., 2014). CSR activities are found to directly affect stakeholders perceptions of organisational justice, fairness and responsibility (Collier and Esteban, 2007; Galbreath, 2010; Kim et al., 2021). In this way, Corporate Social Privacy activities are likely to demonstrate that an organisation endorses the principle of fairness, and thus heighten perceptions of organisational justice and responsibility.

Thus, the research model in Study Two holds that consumers who perceive that organisations are acting responsibly in terms of their NMPv activities show less privacy concern i.e., NMPv activity that signals high levels of justice is expected to be negatively related to privacy concerns. This leads to the following set of hypotheses:

Hypothesis 1: An organisation's reported NMPv activities signalling high levels of control are positively related to privacy concern.

Hypothesis 2: An organisation's reported NMPv activities signalling high levels of justice are negatively related to privacy concern.

3.5.2.2 Nonmarket Privacy Activities and Consumer Trust

Control and justice are found to influence trust in the nonmarket literature (DenHond et al., 2014; Liedong et al., 2014) and are also found to influence trust in the privacy literature

(Greenaway et al., 2015; Lwin et al., 2007). Lwin et al. (2007) argue that where consumers perceive that organisations are acting responsibly, this will lead to greater consumer trust. Privacy activities that reflect values of justice build consumer trust in the organisation, where consumers feel they have little control (Culnan and Armstrong, 1999). It is therefore expected that levels of control and justice associated with NMPv activities will influence consumer trust in an organisation.

Just as privacy activities reflecting justice engender increased consumer trust, so too should NMPv activities that reflect justice. Nonmarket environment activities that reflect values of justice have been found to equalise control imbalances and increase organisational trust (DenHond et al., 2014; Liedong et al., 2014). Thus, organisations who act responsibly, in terms of their nonmarket activities, experience greater consumer trust (Liedong et al., 2014). Positive perceptions of an organisation's nonmarket activities most often associated with CSR activities, have been found to lead to increased consumer trust (Castaldo et al., 2009; Choi and La, 2013; Martínez and del Bosque, 2013). This is most likely because nonmarket activities that reflect values of justice are associated with signalling integrity (Park et al., 2014) and benevolence (Hess, 1995). The violation of integrity and benevolence can lead to reduced trust (Bansal and Zahedi, 2015). However, for CPA benevolence is often missing (Liedong et al., 2014), as organisations traditionally participate in lobbying as a reaction to issues that directly affect only themselves (Hillman and Hitt, 1999). In this way, lobbying is typically egocentric, with benefits accruing only to the organisations that pursue it (Kim, 2008) and enables organisations to control their nonmarket environment conditions (Bauer, 2015). As discussed in Section 2.3.2, organisations can also lobby with the aim of resolving public or social issues. Such lobbying is referred to as responsible lobbying/deliberative lobbying (Lock and Seele, 2017). Deliberate lobbying expresses more of the altruistic values of CSR, reflecting perspectives of Political CSR (Lock and Seele, 2017). It would be expected that this type

of lobbying, demonstrating responsibility and justice, would engender increased levels of trust similar to traditional Political CSR activities.

Thus, in this research, it is posited that consumers who perceive that organisations are acting responsibly in terms of their NMPv activities, are expected to have increased consumer trust. Regardless of whether the NMPv activity is shaped as a CSR or a CPA activity, it is the levels of control or justice signalled by those NMPv activities that are expected to influence levels of consumer trust. This leads to the following set of hypotheses:

Hypothesis 3: An organisation's reported NMPv activities signalling high levels of control are negatively related to consumer trust.

Hypothesis 4: An organisation's reported NMPv activities signalling high levels of justice are positively related to consumer trust.

3.5.2.3 Nonmarket Privacy Activities and Consumer Intentions

Control and justice have been found to influence a consumer's intentions in both the privacy literature and the nonmarket literature. Control, for example, has been found to influence a consumer's intentions to accept or use a system (Rust et al., 2002). Justice in turn, has been found to influence consumers' intentions where nonmarket environment activities violate integrity and benevolence (Bansal and Zahedi, 2015). How an organisation demonstrates socially responsible or ethical behaviour influences a consumer's purchase intention (Creyer, 1997). Where organisations' nonmarket activities are not seen to be just, it can lead to negative consumer responses such as reduced intentions (Liedong et al., 2014). It is expected that levels of control and justice, signalled by an organisation's NMPv activities, will influence a consumer's intentions, including intentions to purchase a product or service, or to continue use of a system or service.

Intentions to accept/purchase or continue, are most often shaped as outcomes of privacy concerns (Anic et al., 2019; Fortes and Rita, 2016) or outcomes of trust (Hajli et al., 2017; Hong and Cho, 2011; Pavlou and Gefen, 2004). For example, privacy concern has been shown to result in a wide range of privacy-protective and defensive response behaviours (Anic et al., 2019; Son and Kim, 2008) and has been found to reduce an individual's intentions to continue to use a system and increase intentions to protect, withhold or falsify data (Bandara et al., 2020; Krishen et al., 2017; Lwin et al., 2007). If levels of control and justice signalled by NMPv activities influence privacy concern and trust, and privacy concern and trust are found to influence the consumer's intentions, it seems reasonable to expect that NMPv activities will influence consumer intentions to purchase or to continue use of a system. Therefore, in Study Two it is hypothesised that levels of control and justice signalled by an organisation's NMPv activity directly influences a consumer's intention to purchase or continue use of a product/service.

Thus, it is expected that when organisations are perceived by consumers to be acting responsibly in terms of their NMPv activities, the consumers purchase intention/continuance intention will be positively influenced. High-control NMPv activities are therefore expected to have a negative influence on these intentions. This leads to the third set of hypotheses:

Hypothesis 5: An organisation's reported NMPv activities signalling high levels of control are negatively related to purchase intention/continuance intention.

Hypothesis 6: An organisation's reported NMPv activities signalling high levels of justice are positively related to purchase intention/continuance intention.

3.5.2.4 Privacy Awareness as Moderator between NMPv and Consumer Responses

Moderation explains how the strength or direction of the relationship between two constructs is altered, due to the presence of a third variable or a moderator variable (Hair et al., 2017) i.e., the relationship between two variables is changed by the moderator. The importance of moderation is that it accounts for heterogeneity in the data. This research explores privacy awareness as a moderator of the relationship between NMPv activities and consumer responses. Many privacy studies consider 'awareness' as a key dimension influencing privacy concern e.g., Internet Users Information Privacy Concern (Malhotra et al., 2004), and Internet Privacy Concern (Hong and Thong, 2013). However the type of 'awareness' considered in these studies is the user's awareness of how the data will be collected, used, shared, stored etc. Another type of awareness found to influence privacy concern is social privacy awareness (Dinev and Hart, 2006). Individuals with high social privacy awareness will closely follow issues related to privacy, including practices, policies, and consequences of any potential privacy violations (Dinev and Hart, 2006). Benamati et al. (2017) posit that privacy awareness consists of two dimensions of prior experience of privacy and media exposure. However, as privacy legislation regimes are so complex, particularly in the US where each state has its own specific privacy regulations, many consumers are not aware of, or understand, the complex responsibilities of organisations or their own rights. In this research, privacy awareness is defined as the understanding of the possible implications that an organisation's policies and/or privacy regulation holds for preserving privacy, i.e., that the consumer understands privacy practices, privacy legislation, the use of disclosed information, and privacy legislation (Warner and Wang, 2019).

Consumers can respond to NMPv activities in a number of ways. For example, by deciding not to continue to engage with the organisation, or deciding not to purchase a product or service from the organisation, or by withholding information or by falsifying it. However,

the relationship between an organisation's NMPv activities and the consumer's response is expected to be moderated by the consumer's level of privacy awareness (Warner and Wang, 2019). In other words, where a consumer fully understands privacy obligations, privacy rights and the implication of privacy for society – they are expected to respond more negatively to say, an organisation lobbying for reduced privacy rights, than a consumer with little privacy awareness. Warner and Wang (2019) found that users with higher privacy awareness responded to certain privacy activities with higher privacy concerns than users with low privacy awareness and lower levels of consumer trust. The moderation effect can be explained by PRE Theory, where the 'privacy aware' consumer will interpret the privacy activity as demonstrating too much power and not enough responsibility, and therefore respond more negatively. The consumer who is not privacy aware will interpret the privacy activity as more balanced, and respond less negatively.

In this way, a consumer with high levels of privacy awareness, is expected to respond to privacy activities with more privacy concern, less consumer trust, and less purchase intention/continuance intention than a consumer with low levels of privacy awareness. Thus, privacy awareness is expected to moderate the relationship between NMPv activities and a consumer's response. This leads to the following set of hypotheses:

Hypothesis 7: Privacy awareness positively moderates the relationship between NMPv activities and privacy concern, such that the relationship is stronger when privacy awareness is high than when it is low.

Hypothesis 8: Privacy awareness negatively moderates the relationship NMPv activities and consumer trust, such that the relationship is stronger when privacy awareness is low than when it is high.

Hypothesis 9: Privacy awareness negatively moderates the relationship between NMPv activities and continuance intention, such that the relationship is stronger when privacy awareness is low than when it is high.

3.6 Summary and Next Steps

This chapter presented the proposed research framework(s) and the hypothesised relationships in these frameworks. Table 3.2. presents the hypothesised relationships in Study Two.

Table 3.2 Summary of Hypothesised Relationships in Study Two

H1:	An organisation's reported NMPv activities signalling high levels of control are positively related to privacy concern.
H2:	An organisation's reported NMPv activities signalling high levels of justice are negatively related to privacy concern.
H3:.	An organisation's reported NMPv activities signalling high levels of control are negatively related to consumer trust.
H4:	An organisation's reported NMPv activities signalling high levels of justice are positively related to consumer trust.
H5:	An organisation's reported NMPv activities signalling high levels of control are negatively related to purchase intention/continuance intention.
H6:	An organisation's reported NMPv activities signalling high levels of justice are positively related to purchase intention/continuance intention.
H7:	Privacy awareness positively moderates the relationship between NMPv activities and privacy concern, such that the relationship is stronger when privacy awareness is high than when it is low.
H8	Privacy awareness negatively moderates the relationship between NMPv activities and consumer trust, such that the relationship is stronger when privacy awareness is low than when it is high.
H9:	Privacy awareness negatively moderates the relationship between NMPv activities and continuance intention, such that the relationship is stronger when privacy awareness is low than when it is high.

This research addresses a number of gaps in the literature and improves our understanding of privacy in the nonmarket environment. The Nonmarket Privacy Orientation Matrix and the Nonmarket Privacy Activities Codebook, developed in Study One, meet calls to construct a mechanism that is 1) characterised by the levels of control or justice signalled by an organisation's privacy activities; and 2) that can be used to position an organisation's privacy orientation (Greenaway et al., 2015). The Nonmarket Privacy Orientation Matrix and the Nonmarket Privacy Activities Codebook are used to qualitatively explore the NMPv activities of a sample of organisations, in terms of the levels of control and justice signalled by them. The data is then used to position their nonmarket privacy orientation accordingly. The research model developed for Study Two addresses calls for power-based approaches to nonmarket environment research (Frynas et al., 2017), by examining the

relationship between NMPv activities and consumer outcomes, using PRE Theory. The hypothesised relationships in the research model for Study Two are quantitatively investigated. The methodologies for Study One and Study Two are outlined in Chapter Four.

4 CHAPTER FOUR: RESEARCH METHODOLOGY

4.1 Introduction

This chapter details the overall methodological approach of this research. The chapter starts by reiterating the key hypotheses, in order to situate the methodological discussion. Then, a brief discussion of the philosophical assumptions underlying the research, and an introduction to mixed methods research is presented. The next section focuses on the specific research design approach chosen. The appropriateness of a mixed methods approach, which provides support for an exploration of NMPv using a combination of quantitative survey based research and qualitative secondary data based research, is then described. Next, an overview of the sampling strategies, data collection processes, and data analysis strategies and quality criteria for each of the two separate studies, is presented. Ethical considerations are then discussed, and the chapter concludes with a discussion of the integration of the methods used.

4.2 Research Overview

The overall goal of this research is to develop a deeper understanding of privacy in the nonmarket environment, which is a nascent and little explored phenomenon. To achieve this aim, the three research questions outlined in Section 1.4 are developed. In Study One, RQ1 and RQ2 are addressed qualitatively. First, a taxonomy is developed to code NMPv activities in terms of the levels of control and justice signalled by them. As many empirical research studies analyse CSR reports in respect of one or more categories of social, environmental or ethical matters (Unerman, 2000), the framework is then qualitatively applied to a sample of organisations CSR reports in order to determine their NMPv

orientation. Then Study Two is concerned with addressing RQ3 quantitatively using an experimental vignette-based survey. The following hypotheses are formulated in order to address RQ3:

H1: An organisation's reported NMPv activities signalling high levels of control are positively related to privacy concern.

H2: An organisation's reported NMPv activities signalling high levels of justice are negatively related to privacy concern.

H3: An organisation's reported NMPv activities signalling high levels of control are negatively related to consumer trust.

H4: An organisation's reported NMPv activities signalling high levels of justice are positively related to consumer trust.

H5: An organisation's reported NMPv activities signalling high levels of control are negatively related to purchase intention/continuance intention.

H6: An organisation's reported NMPv activities signalling high levels of justice are positively related to purchase intention/continuance intention.

H7: Privacy awareness positively moderates the relationship between NMPv activities and privacy concern, such that the relationship is stronger when privacy awareness is high than when it is low.

H8 Privacy awareness negatively moderates the relationship between NMPv activities and consumer trust, such that the relationship is stronger when privacy awareness is low than when it is high.

H9: Privacy awareness negatively moderates the relationship between NMPv activities and continuance intention, such that the relationship is stronger when privacy awareness is low than when it is high.

An overview of the research approach is discussed in the next section of this chapter.

4.3 Research Approach

The approach to research may be largely dependent on the researcher's philosophical assumptions (Denzin and Lincoln, 2011) and how they influence the research aims and research questions. Therefore, this section first presents the key research philosophies in

business and management research, then outlines the research assumptions associated with those philosophies, and finally discusses the selected philosophical perspectives of this research, and the rationale for those selections. This section concludes with an outline of the proposed research methodological approach and the rationale for its selection.

4.3.1 Research Philosophies and Assumptions

Research is typically influenced by the researcher's philosophical foundations; therefore it is important to understand and acknowledge the philosophical perspectives that the researcher brings to their study (Creswell and Plano Clark, 2007). Johnson and Clark (2006) argue that business and management researchers need to be aware of their research philosophy, as it will influence how researchers understand what they are investigating, and influence the selection of research methodology (Gill and Johnson, 2002). According to Saunders et al. (2015), the business and management sciences have focused on five major research philosophies: positivism/postpositivist, critical realism, constructivism/interpretivism, postmodernism and pragmatism. The beliefs underpinning research philosophies are referred to as philosophical assumptions (Crotty, 1998), as research paradigms (Lincoln et al., 2011; Mertens, 2010), and as broadly conceived research methodologies (Neuman, 2009), and as alternative knowledge claims (Creswell, 2009). For the purpose of this research, these philosophical beliefs are referred to as research paradigms; namely, ontology, epistemology and axiology. By way of background, a summary of these paradigms and their associated research philosophies for business and management research, is presented in Table 4.1, as per Saunders et al. (2015), followed by a brief overview of them.

Table 4.1 Philosophical Assumptions in Business and Management Research (Saunders et al., 2015)

Ontology	Epistemology	Axiology	Typical Research Methods
	Positivism/Postpositivism		
• Real, external, dependent. • One true reality (universalism) • Granular, ordered	• Scientific method • Observable and measurable facts • Law-like generalisations • Causal explanation and prediction as contribution	• Value-free research • Researcher is detached, neutral and independent of what is researched • Researcher maintains objective stance • Researcher is biased (postpositivism)	• Typically deductive, highly structured, large samples • Typically quantitative methods, but range of data can be analysed (postpositive)
	Critical realism		
• Stratified/layered (the empirical, the actual and the real) • External, independent • Objective structures • Causal mechanisms	• Epistemological relativism • Knowledge historically situated and transient • Facts are social constructions • Historical causal explanation as contribution	• Value-laden research • Researcher acknowledges historically situated bias by world views • Researcher tries to minimise bias and errors • Researcher is as objective as possible	• Retroductive, in-depth historically situated analysis of pre-existing structures and emerging agency • Range of methods and data types to fit subject matter
	Constructivism/ Interpretivism		
• Complex, rich, socially constructed through culture and language • Multiple meanings, interpretations, realities • Flux of processes, experiences, practices	• Theories and concepts focus on narratives, stories, perceptions and interpretations • New understandings and worldviews as contribution	• Value-bound research • Researchers are part of what is researched • Subjective, reflexive - researcher interpretations key to contribution	• Typically inductive • Small samples • In-depth investigations - qualitative methods of analysis, but a range of data can be interpreted
	Postmodernism		
• Nominal • Complex, rich, socially constructed through power relations • Some meanings, interpretations, realities are dominated and silenced by others • Flux of processes, experiences, practices	• What counts as 'truth'/ 'knowledge' decided by dominant ideologies • Focus on absences, silences and oppressed/ repressed meanings, interpretations and voices • Exposure of power relations, challenge of dominant views as contribution	• Value-constituted research • Researcher/research embedded in power relations • Some research narratives repressed/ silenced at expense of others • Researcher radically reflexive	• Typically deconstructive – reading texts and realities against themselves • In-depth investigations of anomalies, silences and absences • Range of data types, typically qualitative methods of analysis
	Pragmatism		
• Complex, rich, external 'reality' is the practical consequences of ideas • Flux of processes, experiences and practices	• Practical meaning of knowledge in specific contexts • 'True' theories and knowledge are those that enable successful action • Focus on problems, practices and relevance • Problem solving and informed future practice as contribution	• Value-driven research • Research initiated and sustained by researcher's doubts and beliefs • Researcher is reflexive	• Following research problem and research question • Range of methods: mixed, multiple, qualitative, quantitative • Action research - emphasis on practical solutions and outcomes

In business and management research**, ontology** is associated with a central question of whether social entities should be perceived as objective or subjective (Saunders et al., 2015). **Epistemology** can be defined as the criteria by which the researcher classifies what does and does not constitute knowledge (Hallebone and Priest, 2009). **Axiology** is the study of the theory on the nature of value (Heron and Reason, 1997), incorporating questions about how we, as researchers, deal with both our own values and those of our research participants (Saunders et al., 2015).

Whilst **positivism** contends there is a single reality thus seeking to identify causal relationships through objective quantitative measurement (Antwi and Hamza, 2015; Firestone, 1987), **post-positivists** reject the idea that any individual can see the world perfectly as it really is. Positivism and post-positivism are more often aligned to quantitative methods of data collection and analysis (Guba, 1990, Denzin and Lincoln, 2011). **Critical-realism** focuses on explaining what we see and experience, in terms of the underlying structures of reality that shape the observable events. The axiological position is that knowledge of reality is a result of social conditioning that must consider the social actors involved. Reality is viewed as the most important philosophical consideration (Fleetwood, 2005; Saunders et al., 2019) and thus a range of methods is acceptable (Reed, 2005). **Constructivism/interpretivism** contends that there is no such thing as objective reality, pointing instead to a subjective reality based on multiple realities of different observers (Lee, 1991; Saunders et al., 2015). An axiological implication of this is that interpretivists/constructivists recognise that their own values and beliefs play an important role in the research process. **Postmodernism** emphasises the role of language and of power relations, seeking to question accepted ways of thinking and give voice to alternative marginalised views (Saunders et al., 2019). They reject the modern objectivist, realist ontology of things, and instead emphasise chaos and change, and how order can only be brought about through our language (Chia, 2003). Finally, **pragmatism** finds its

philosophical foundation in the historical contributions of the philosophy of pragmatism (Maxcy, 2003; Saunders et al., 2019) and contends that researchers should use the philosophical and methodological approach that works best for the particular research problem that is being investigated (Tashakkori and Teddlie, 1998).). Pragmatism is often associated with mixed-methods or multiple-methods (see Creswell and Plano Clark, 2011; Johnson and Onwuegbuzie, 2004; Teddlie and Tashakkori, 2008), where the focus is on the consequences of research and on the research questions rather than on the methods.

Philosophical positions about epistemology, ontology and axiology, exert significant influences on the methodological approach to be used in a research project (Antwi and Hamza, 2015; Morgan, 2007). Choosing the methodological approach for research is important, as the methodological implications of paradigm choice permeate the research questions, participant selection, data collection instruments and collection procedures, as well as data analysis. Pragmatism was selected as the philosophical approach for this research, and mixed methods was selected as the methodological approach. In the remainder of this section, the rationale for these choices is discussed.

4.3.1.1 Philosophical Approach - Rationale

Pragmatism was chosen for four key reasons. First, pragmatism aims to find the middle ground between philosophical dogmatism, and is therefore more useful than research philosophies that lay a sole emphasis on abstraction or philosophical theory-generation (Johnson and Onwuegbuzie, 2004). Second, the axiological assumptions of the researcher are that everyone values privacy and that privacy is important to society. This of course may not be the case. Addressing the potential for bias, pragmatism serves as a rationale for greater rigour in research (Mitchell, 2018) and allows the research to undergo a continuous cycle of inductive, deductive, and when appropriate – abductive, reasoning. In this way, pragmatists often treat "truth" as the final outcome of scientific inquiry, meaning that

something cannot be true unless it is potentially observable (James and Gunn, 2000). Third, pragmatism allows the researcher in this study to be open to adopt a 'what works best' approach to provide the deepest conceptualisation and understanding of the nonmarket privacy phenomena, and to use whatever methodology worked best and provide a balance of subjectivity and objectivity throughout the research. Finally, the philosophical assumptions of pragmatism seemed most appropriate for privacy research in two key areas; namely epistemology and methodology. Epistemologically, pragmatism is premised on the idea that research should avoid getting mired in metaphysical debates about the nature of truth and reality and focus instead on concrete, real-world issues (Kelly and Cordeiro, 2020; Patton, 2015) such as privacy. As NMPv is still quite nascent and relatively unexplored, methodologically, NMPv can be more comprehensively understood leveraging the different methodological approaches encouraged by pragmatism.

On a philosophical level, pragmatism supports the view that while qualitative and quantitative methods are distinct, they are also commensurate as both advanced knowledge production (Bishop, 2015) and shared meaning making (Shannon-Baker, 2015). This however raises some methodological concerns. For instance, if a research problem has different approaches, how can they be measured or observed (Feilzer, 2010) and how can results be integrated? Certainly, one important strategy for inquiry would be to employ multiple methods, measures, and perspectives (Patton, 2015). Methodologically, pragmatic researchers are better equipped to deal with complex, dynamic social processes where action, even if carefully planned, can have varied outcomes. This is because they can draw on both qualitative and quantitative methods. Although pragmatism supports the use of mixed methods, it is important to note that, for pragmatists, the best method is the one that is most effective in producing the desired consequences of the inquiry, whether it is a single-method, multiple methods, or a mix of methods (Tashakkori and Teddlie, 2008).

4.3.1.2 Methodological Approach - Rationale

There are three types of approaches to research, namely qualitative, quantitative and mixed methods (sometimes referred to as 'the third methodological movement'). This research adopts a mixed methods approach. Mixed methods is the class of research designs where the researcher mixes or combines quantitative and qualitative research techniques, methods, approaches, concepts or language into a single study for the purpose of breadth and depth of understanding and corroboration (Yu and Khazanchi, 2019). Mixed methods is capable of bridging the divide between the quantitative and qualitative positions (Johnson and Onwuegbuzie, 2004). In mixed methods, research is not restricted by the use of traditional approaches to data collection but is guided by a foundation of enquiry that underlies the research activity (Creswell, 2015). Such an approach enables researchers to develop a more in-depth understanding of a phenomenon (Venkatesh et al., 2013). By combining quantitative and qualitative methods, mixed method studies offset the weaknesses inherent in single method studies (Creswell and Plano Clark, 2007). Creswell and Plano Clark (2007) argue that mixed methods research helps address research questions that cannot be explored by quantitative or qualitative methods alone and provides a greater repertoire of tools to meet the aims and objectives of a study. Mixed methods can also facilitate both the confirmation of hypotheses and theory through quantitative methods, and the generation of theory, or generation of items for inclusion in a questionnaire through qualitative methods (Teddlie and Tashakkori, 2009). Mixed methods can also help to develop stronger inferences from data, and to present divergent views which force the re-examination of assumptions underlying the qualitative and quantitative components of a study (Tashakkori and Teddlie, 2008; Timans et al., 2019).

Mixed methods was selected as the methodological approach for this research, primarily because the research questions are varied, drawing on a range of disciplines, and are characterised by investigations involving multiple levels of analysis (Currall and Towler,

2003). Thus, there is benefit in combining the complementary strengths of quantitative and qualitative approaches. Additionally, the mixed method approach offers a rich research design strategy for studying emergent complexities and interactions inherent in IS phenomena (Yu and Khazanchi, 2019). The most commonly identified justifications for the use of mixed methods according to Doyle et al. (2009) are presented in Table 4.2 together with the rationales justifying the choice of mixed methods in this research.

Table 4.2 Rationale for Mixed Methods

(Source: Doyle et al., 2009)

Rationale	***Description***	***The Rationale in This Research***
Exploration:	An initial phase is required to develop an instrument or intervention, identify variables to study or develop a hypothesis that requires testing.	Combining our limited understanding of consumer responses to privacy activities in the nonmarket environment, the nascence of privacy in the nonmarket environment, and the extension of constructs and theories to this context for the first time.
Completeness:	Provides a more comprehensive account of phenomena under study.	This research aims to develop a comprehensive understanding of privacy in the nonmarket environment, which is a nascent and little explored phenomenon.
Different Research Questions:	Both quantitative and qualitative questions may be posed at the beginning of the study in addition to mixed methods questions (Creswell, 2015).	The differing research questions RQ1, RQ2, and RQ3 justify a mixed methods approach.
Triangulation **(convergence)**	Using quantitative and qualitative methods so that findings may be mutually corroborated.	
Expansion:	The first phase has findings that require explanation qualitatively.	
Offset Weaknesses:	Ensures that weaknesses of each method are minimised (Creswell, 2015).	
Illustration:	Qualitative data are used to illuminate quantitative findings (Bryman, 2012).	

Methodological purists argue against the combination of quantitative and qualitative approaches, in the belief that quantitative and qualitative research methods cannot be mixed in a single study as they have such different ontological and epistemological origins (Doyle et al., 2016). However, Johnson and Onwuegbuzie (2004) argue that positivist and

non-positivist philosophies lie on an epistemological continuum with mixed methods research occupying the middle ground.

Epistemologically, findings are generated through interaction between researcher and data using a logic of inquiry that includes the use of induction e.g., discovery of patterns, deduction e.g., testing of theories and hypotheses, and abduction e.g. uncovering and relying on the best of a set of explanations for understanding one's results (Johnson and Onwuegbuzie, 2004; Onwuegbuzie et al., 2010; Yu and Khazanchi, 2019). Ontologically, mixed research methods adopt a belief in realism i.e., "all theories are approximations, where researchers recognise the existence and importance of the natural or physical world as well as the emergent social and psychological world" (Johnson and Onwuegbuzie, 2004, p.18). This thinking incorporates methodological pluralism, which frequently results in superior research compared to monomethod research (Johnson and Onwuegbuzie, 2004; Johnson et al., 2007).

Advocates of mixed methods (Creswell and Plano Clark, 2011; Johnson and Onwuegbuzie, 2004; Timans et al., 2019) recognise that, despite its several advantages, mixed methods can also present several problematic concerns, and these issues are summarised in Table 4.3, alongside the advantages of mixed methods. The primary disadvantage of mixed methods relates to the greater time, resource and effort required (Ivankova et al., 2006) and the complexities of describing the connection between the studies (Tashakkori and Creswell, 2007).

Table 4.3 Advantages and Disadvantages of Mixed Methods

Advantages of Mixed Methods	Disadvantages of Mixed Methods
- Words, pictures and narratives can be used to add meaning to numbers – quantitative research is weak in understanding context. - Numbers can be used to add precision to words, pictures and narrative. - Qualitative research has difficulties generalizing. - Can draw on strengths from both quantitative and qualitative research - where the strength of one method can be applied to overcome the weaknesses of another. - Can provide more complete knowledge and stronger conclusions through convergence and corroboration of findings. - Provides the opportunity for both generating and testing theory.	- Can be difficult for one researcher to carry out – especially in case of parallel designs. - Includes weaknesses of both qualitative and quantitative research. - Time-consuming. - Expensive. - A challenge to learn and master multiple methods. - Problems of paradigm mixing - methodological purists who hold that one should always work within either a qualitative or a quantitative paradigm. - Problem of convincing others of validity.

4.4 Research Design and Strategy

The research design is the plan that structures the investigation to explore the research questions, and the research strategy is the method used to implement that plan (Punch, 2005). Good research design ensures that the research strategy chosen will help the researcher more effectively conclude the research question(s). Mixed methods studies are often critiqued for failure to adequately explain the plan for research design for all aspects of the research (Venkatesh et al., 2013). By following the Good Reporting of a Mixed Methods Study (GRAMMS) method outlined by O'Cathain et al. (2008), this research hopes to overcome this weakness. Table 4.4 outlines the key steps from GRAMMs, and details where they are addressed in this chapter.

Table 4.4 How GRAMMS are Addressed in this Research

GRAMMS	Where the step is addressed
Describes the justification for using mixed methods research to the research question.	Section 4.3.1.2
Describes the mixed methods design in terms of the purpose, priority and sequence of methods.	Section 4.4.1 (Purpose) Section 4.4.2 (Priority and Sequence)
Describes each method in terms of sampling, data collection and analysis.	**Study One** Section 4.6.1 (Sampling) Section 4.6.2 (Design and Data Collection) Section 4.6.3 (Analysis) **Study Two** Section 4.7.1 (Sampling) Section 4.7.2/4.7.3 (Design and Data Collection) Section 4.7.4 (Analysis)
Describes the integration of the quantitative and qualitative components.	Section 4.8

4.4.1 Research Design: Methods of Inquiry

Firstly, in accordance with pragmatism, the most appropriate methods of inquiry to address the research questions are chosen. These methods are derived from the typology of research purposes developed by Newman et al. (2003), which suggests that methods of inquiry should be based on the purposes of the research. The overarching purpose of this research, as outlined previously in Section 1.2, is to develop a more comprehensive understanding of privacy in the nonmarket environment. Given the nascency of privacy in the nonmarket environment, this research first seeks to 'generate new ideas' regarding NMPv orientations. Such a purpose is traditionally addressed through a qualitative method (Newman et al., 2003). In this research, this is achieved using secondary data - more specifically, CSR Reports. The research also seeks to explore proposed relationships, a purpose which is typically undertaken using a quantitative method (Newman et al., 2003). In this research, this is achieved using an experimental survey.

4.4.2 Research Design: Priority and Sequence of Mixed Methods

This section presents a strategy for conducting this research, as required by guidelines on mixed methods research from Venkatesh et al. (2013). Creswell and Plano Clark (2007) developed a typology for mixed methods design strategies, consisting of four main types; namely triangulation, embedded, explanatory and exploratory. The triangulation design strategy is the most well-known design (Creswell et al., 2003), where the quantitative and qualitative phases occur concurrently, with equal weighting. The embedded design is characterised by having one dominant method, whereas the other data set provides a secondary or supportive role (Doyle et al., 2016). Explanatory design consists of two sequential phases (beginning with quantitative and then qualitative) aiming to explain or enhance the quantitative results. The exploratory design is a sequential design where the first study i.e., the qualitative study, helps in the development of the second study i.e. the quantitative study.

Study One is a qualitative study, involving the thematic analysis of a sample of organisations' NMPv activities from their CSR publications, in order to position their NMPv orientation. In thematic analysis, the themes can be established using grounded theory and the researcher's immersion in the coding data, or a codebook can be used (Braun and Clarke, 2006). The latter approach is applied in Study One. The first stage of Study One is thus focused on developing the codebook. Due to the geographically dispersed panel, the Online Delphi Survey method was adopted to develop the codebook. The Online Delphi Survey method (sometimes referred to as an E-Delphi) is characterised by involving groups of experts without concern for geography, to reply anonymously to a number of iterative rounds of specific survey questions to achieve group consensus (Linstone and Turoff, 2002). The Online Delphi Survey method is difficult to situate in a methodological category (Sekayi and Kennedy, 2017) and has been described as a

qualitative, quantitative, and mixed methods approach to research (Sekayi and Kennedy, 2017).

Study One thus takes an embedded design approach, where the Online Delphi Survey provides a supportive role to the analysis of the CSR reports. Study Two, then involves two experiments, using experimental vignette surveys, aimed at exploring a number of hypotheses regarding the influence that NMPv activities have on privacy concern, consumer trust and purchase intention/continuance intention. In this way, the overall research design takes an exploratory design approach, characterised by a qualitative study building to a quantitative study. In this way, the overall research is described as an embedded-exploratory sequential-dependent design.

Creswell and Plano Clarke (2007) also suggest a number of key considerations that are important to the mixed methods design approach, namely Timing, Weighting, and Integration and these are presented in Table 4.5, together with how these considerations are applied in this research.

Table 4.5 Considerations Important to Mixed Methods Design

(Source: Creswell and Plano Clarke, 2007)

	Options	**Differences**	**In This Research**
Timing	Sequential/ Concurrent	In a *sequential design*, the quantitative component precedes the qualitative component, or vice versa. In *concurrent design*, both components are executed (almost) simultaneously (Guest, 2013). Two research components are considered *dependent* if the implementation of the second component depends on the results of data analysis in the first component (Guest, 2013).	Study Two follows on from Study One and is dependent on the results of Study One. In this way, the research activities are said to be sequential-dependent.
Weighting	QUAN/QUAL or qual/QUAN or QUAL/quan	Weighting in an exploratory design depends on the purpose of its utilisation; if used to develop a theory, the qualitative phase is normally dominant but if used to develop and test an instrument the quantitative phase usually takes priority (Creswell and Plano Clark, 2011). Weightings are depicted visually using uppercase for dominant components and lowercase for minor components (Teddlie and Tashakkori, 2009).	The priority weighting in this design was given to Study Two – the quantitative survey method - because Study Two represented the major aspect of data collection and analyses in the research. In this way, Study One is represented as 'qual' and Study Two is represented as 'QUAN'.
Integration:	Design/ Methods/ Reporting	Integration can occur at the design level, or by integrating methods, or by integrating results at the interpretation/reporting stage.	**Design:** results from the ODS are fully integrated into the qualitative analysis of Study One. **Methods:** results from the ODS inform the survey used in the EVM of Study Two, and therefore adopts the 'building' approach to methods integration. **Interpretation and Reporting:** the data from both studies are jointly discussed through the reporting narrative.

The design is summarised in the following format: **(mixed→qual)→QUAN**. The linear presentation represents a sequential research design, the brackets represent the embedded study, the arrows represent dependence and timing, and the use of capital/lowercase represents weighting. Figure 4.1 illustrates the research design and phases applied in this research.

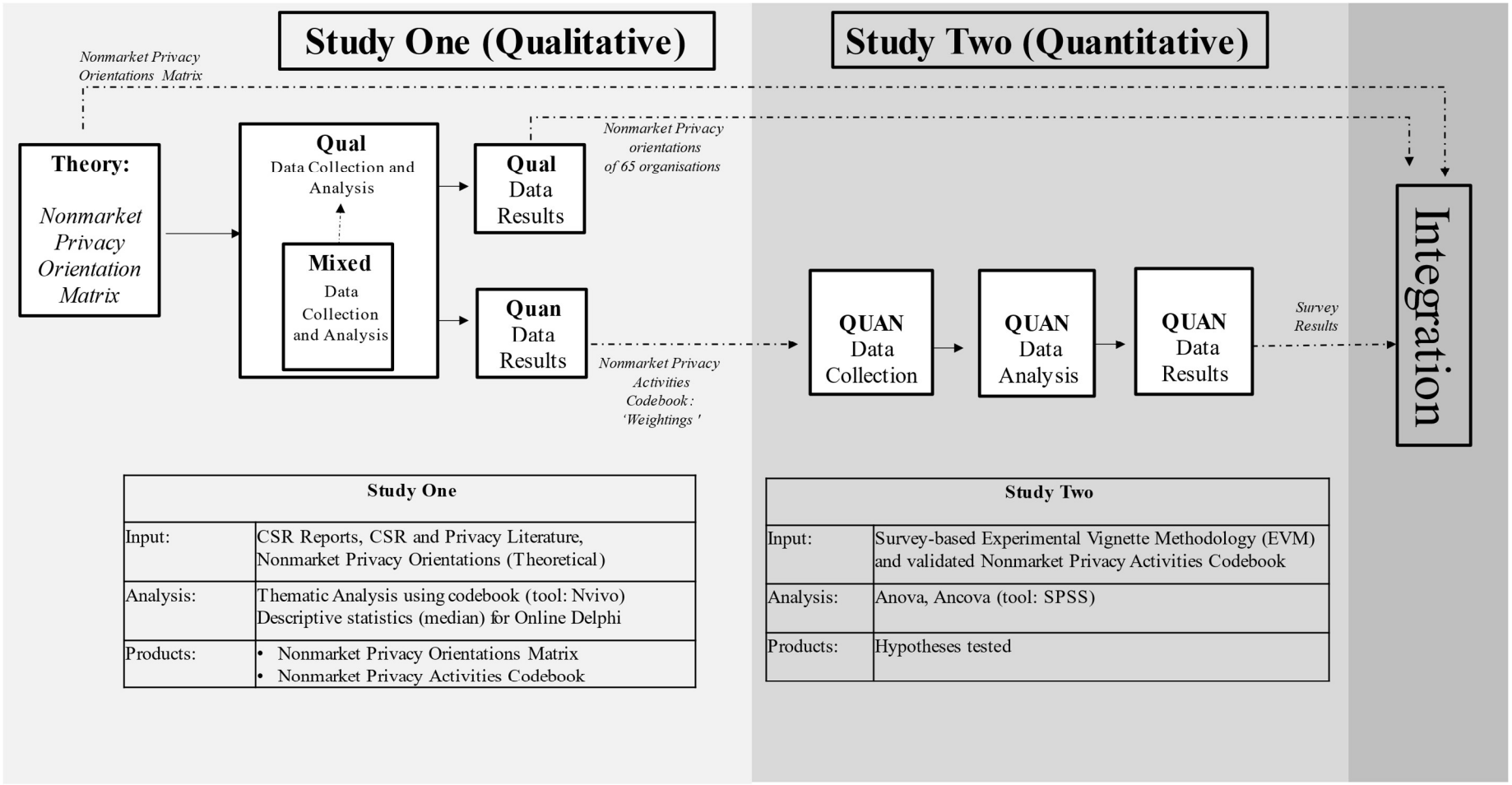


Figure 4.1 Embedded-Exploratory Sequential Design

4.5 Ethical Considerations for this Research

To ensure that the research maintained high ethical standards, applications were submitted for ethical clearance to the university's research ethics committee, for both Study One and Study Two. See Appendix A, K, and M for a copy of these approvals. A number of key ethical considerations were considered for both the Online Delphi Survey in Study One, and the vignette surveys in Study Two, namely anonymity and confidentiality, right to autonomy and informed consent, and right of self-determination (Keeney et al., 2011). Statements of confidentiality and anonymity were included in the cover emails, plain language statements, and the ethics committee approval submission. The plain language statements explained the benefits, rights and risks involved in each study, and consent was secured online at the start of each study. The remainder of this chapter presents a description of the research components of each discrete study, including the research strategy, data collection, preparation and analysis, and the rationale for the analytical techniques applied at each stage.

4.6 Study One

Study One first involves the use of an Online Delphi Survey, and is concerned with addressing the following research question: *RQ1: What are the key privacy activities in the nonmarket environment, and what level of control or justice do these activities signal?*

The results of the Online Delphi Survey forms a codebook which is then applied in the next stage of Study One - the thematic analysis of a sample of CSR reports. This stage is concerned with addressing the following research question: *RQ2: Can an organisation's approach to nonmarket privacy be determined from their published nonmarket privacy activities?*

The steps involved in Study One are outlined in Figure 4.2.

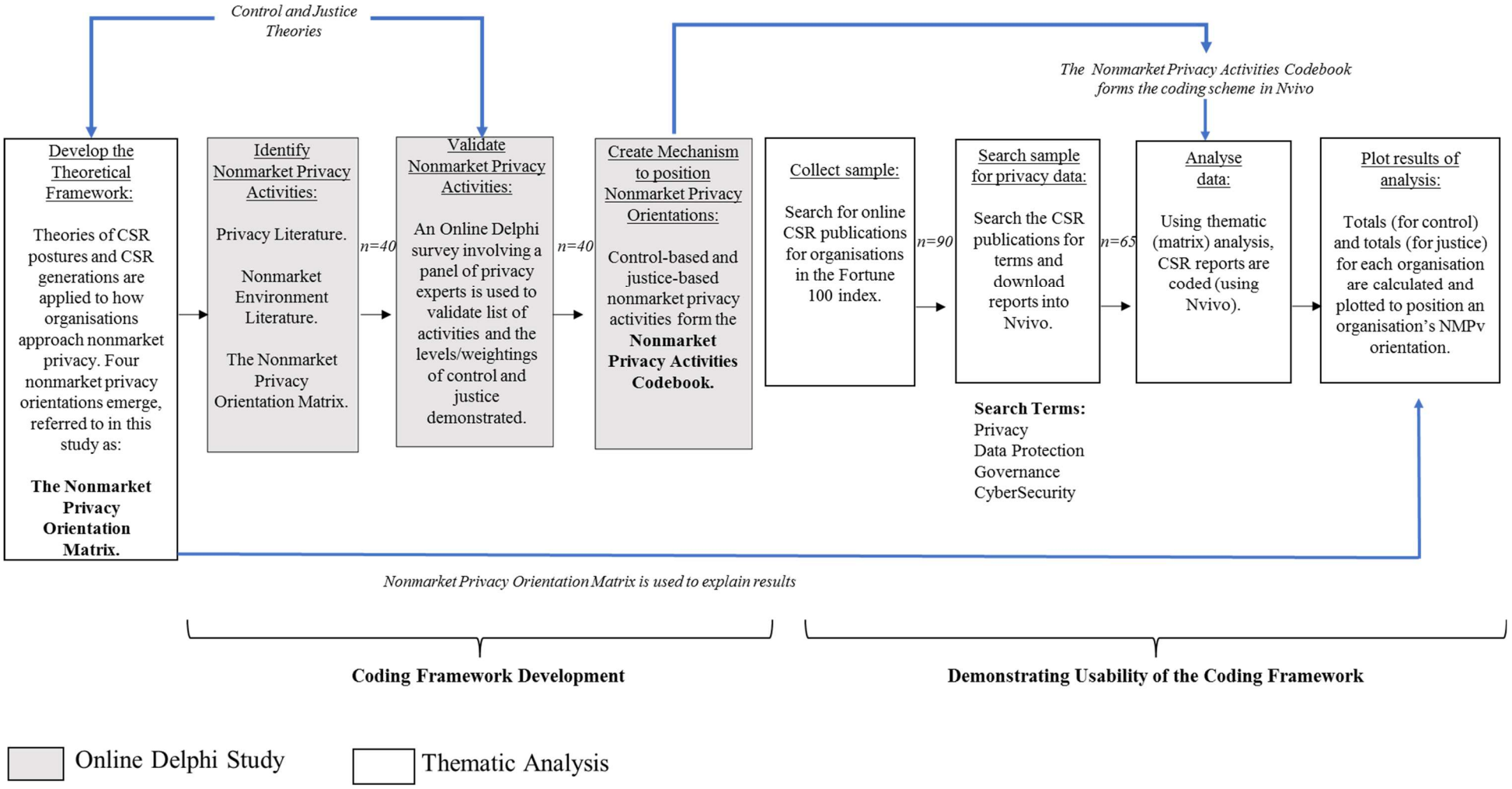


Figure 4.2 Visualisation Of Study One Research

The following section first presents the sampling strategy for both stages of Study One. Following this, the design and data collection of both stages is presented. Then a description of the data analysis is presented, together with the qualitative tools employed for both stages.

4.6.1 Sampling Strategy

Most sampling schemes fall into one of two classes: random sampling schemes, i.e., probabilistic sampling, or non-random sampling schemes, i.e., non-probabilistic sampling (Onwuegbuzie and Collins, 2007; Onwuegbuzie and Johnson, 2006). The vast majority of both qualitative and quantitative studies use non-random samples (Onwuegbuzie and Collins, 2007). A purposive non-random sampling strategy was pursued for both stages of Study One. Purposeful sampling is a technique widely used in qualitative research for the identification and selection of information-rich cases for the most effective use of limited resources (Palinkas et al., 2015). This involves identifying and selecting groups that are especially insightful regarding the phenomenon of interest (Creswell and Plano Clark, 2011; Palinkas et al., 2015). This technique was selected, as the group targeted in the first stage of Study One were representative of experts in privacy. The group targeted in the second stage of Study One were representative of organisations who would typically publish CSR reports. The sampling used in both stages of Study One is described below.

4.6.1.1 <u>Online Delphi Survey Sampling Strategy</u>

This section discusses the sampling strategy for the first stage of Study One, under three main headings; sample size, sample criteria and recruitment, and sample overview.

Sample Size

Whilst Delphi method techniques are typically considered to be surveys, a key difference between Delphi method techniques and the traditional survey is the traditional survey's dependence on a representative sample size (Worrell et al., 2013). This dependency exists because surveys need to enhance the sample population's external validity to the theoretical population of interest and identify statistically significant effects in the sample population (Worrell et al., 2013). Although the Online Delphi Survey method's reliance on expert opinion removes this dependency, generalising the opinions of a non-representative group to a larger population can be problematic (Worrell et al., 2013). However, Worrell et al. (2013) also identify the expert panel having insights above and beyond a representative group, producing potentially fruitful benefits for both research and practice. These experts on the panel are referred to, from here on, as 'panelists'.

If panelists are selected who have similar understanding of the problem of interest, a relatively small sample can be used (Akins et al., 2005). Linstone (1978) argues 7 participants is a suitable minimum panel size in any Delphi study, however the number of panelists depends very much on the topic area as well as the time and resources at the researcher's disposal (Iqbal and Pipon-Young, 2009). Although Delphi studies have been conducted with as many as 1000 panelists, Linstone and Turoff (2002) recommend panels between 10 and 50. Where the background of the Delphi panelist is homogeneous, 10 to 15 experts is sufficient (Delbecq et al., 1975) and can result in useful results (Day and Bobeva, 2005). In a systematic review of Delphi method studies, Boulkedid et al. (2011) found the minimum number of panelists to be 3, the median number to be 17, and the maximum panel size to be more than 400 experts. The majority of Delphi panels are between 15 and 20 respondents (Hsu and Sandford, 2007; Taylor, 2019). In this research, seventeen qualifying panelists were identified, and fourteen agreed to participate.

Sampling Criteria and Recruitment

Purposive sampling is based on the assumptions that a researcher's knowledge about the population can be used to handpick the cases to be included in the sample (Polit and Hungler, 1997). These assumptions are founded on clear inclusion criteria (Patton, 2015). These criteria are applied as a means of evaluating the results and establishing the study's potential relevance to other settings and populations. An expert suitable for a Delphi panel is someone at the top of their field of knowledge, who must be able to see connections between national and international, as well as present and future developments, along with the ability to see connections between different fields of science (Kuusi, 1999; Delbecq et al., 1975).

Due to the importance of the selection process, three sampling criteria were applied to the selection of the Online Delphi Survey panelists. The experts had to (i) be from a country that had strong data protection legislation and national accountability structures in place, such as governance authorities with punitive powers, (ii) have proficiency in the English language and (iii) be able to demonstrate expertise in privacy. However, in order to determine 'expertise' level, exact and explicit criteria are required. Rogers and Lopez (2002) suggest two of five criteria to establish expertness: authorship; conference presentation; member or chair of committee; employed in practice or supervision with specified number of years experience; employed as faculty member with specific interest in an area. For other panels, 'expertness' is assumed on the basis of membership of a particular group or organisation (Campbell et al., 2000). Because this study wanted to evaluate the expertness of both academic and industry participants, the expertise of the panel members in this study was defined in terms of professional accomplishments in multiple domains relevant to privacy, and two of the following five criteria had to be met.

1. Primary or secondary author of two or more privacy related publications concerning privacy from a non-computer science perspective.
2. Three or more presentations on relevant privacy topics at privacy, security, law, data protection, corporate governance, risk, sustainability, government policy, management information systems, socio-political, or ethics conferences.
3. Member/chair of a committee concerned with the delivery and provision of privacy, data protection or digital ethics.
4. Serving as an advisory board member, concerned with data protection, digital ethics, or privacy.
5. Employed as a data protection expert, with at least ten years of work experience.

Once identified, the expert was approached by the researcher via online email or LinkedIn in an attempt to recruit them to the study. The initial contact included an outline of the goals of the project, the commitment requirement and the nature of the inquiry. Delphi methods, such as the Online Delphi Survey method, are unlike other methods, as they require a continued commitment from participants being questioned about the same topic over a number of rounds. Therefore, the need to maintain involvement until the process is completed was also emphasised (Buck et al., 1993). Whitman (1990) found that alongside verbal instruction, written information accompanying the first round enhances effectiveness. So, this information was communicated and repeated in each round. Reminder emails were also sent during each round to enhance response rates.

Sample Overview

An analysis of the participants, and how they met the criteria above is presented in Table 4.6. Seventeen qualifying panelists were identified, where nine of these were academics, and eight were practitioners. Fourteen panelists agreed to participate in the Online Delphi Survey and completed the first round. Twelve panelists completed the second round.

Table 4.6 Subject Matter Experts (SME) Sample Overview

SME	Nationality	Source	Background	University	Expert Selection Criteria
Participated in both rounds					
1	European (Ireland)	Industry	Privacy Practitioner IAPP	N/A	2,5
2	American	Industry/ Academia	Privacy Practitioner Cybersecurity IAPP	North Western University	2,3,4,5
3	American	Industry	Privacy Practitioner Cybersecurity	N/A	1,2,3,5
4	Canadian	Industry	Privacy Practitioner Privacy By Design IAPP	N/A	1,2,5
5	American/ European	Industry/ Academia	Data Protection Law Privacy Research IAPP	Maastricht University	1,2
6	European (Ireland)	Academia	Data Value, Data Research	University College Cork	2,3
7	United Kingdom	Industry	Privacy Practitioner	N/A	2,5
8	European (Ireland)	Industry	Privacy Practitioner IAPP	N/A	2,5
9	European (Ireland)	Academia	Data Protection Law, Privacy Research	University College Dublin	1,2,5
10	European (Holland)	Academia	Privacy and Data Protection Law Privacy Research	Radboud University	1,2
11	United Kingdom	Academia	Privacy Law Privacy Research Privacy Practitioner	Queens University Belfast	2,5
12	European (Ireland)	Industry	Data Protection Law, Risk Management	N/A	2,5
Participated in only the first round					
13	European (Ireland)	Industry	Privacy Law Privacy Policy Digital Ethics	N/A	2,5
14	European (Ireland)	Industry	Privacy Practitioner Data Protection Law IAPP (Board)	N/A	2,3,5
Did not participate					
15	European	Academia	Data Protection	Trinity College Dublin	1,2,5

SME	Nationality	Source	Background	University	Expert Selection Criteria
	(Ireland)		and Privacy Law		
16	European (Italian)	Academia	Privacy Practitioner Privacy Research Data Protection Law	Maastricht University	1,2,5
17	European (Denmark)	Industry	Privacy Awareness Practitioner IAPP	N/A	2,5

4.6.1.2 CSR Reports Sampling Strategy

This section discusses sampling strategy for the CSR reports, under three headings; sample size, sampling criteria and sample overview.

Sample Size

Qualitative studies aim to map out the qualitatively different patterns observed in a data-set rather than to quantify magnitudes. Therefore 'there are no computations or power analyses that can be done in qualitative research to determine a priori the minimum number […] of sampling units required' (Sandelowski, 1995, p. 179). The main goal, Sandelowski argues (p. 183), is to ensure that the sample size is small enough to manage the material and large enough to provide a richly textured understanding, and this is always a matter of subjective judgment. More recent guidelines for thematic analysis (Braun and Clarke, 2013, p. 50) categorise sample size suggestions by the type of data collection and project size. For small projects, 6–10 participants are recommended for interviews, 2–4 for focus groups, 10–50 for participant-generated text and 10–100 for secondary sources. This study uses a sample size of 100 which is in line with sample size guidelines from Braun and Clarke (2013) and aligns with sample sizes used in previous studies exploring CSR reports (e.g., Pollach (2011) analysed 98 CSR reports from organisations in the Forbes 500 and Fortune 2000 listings; Martin et al. (2018) analysed 98 CSR reports of the Fortune 100 organisations; Johnson et al. (2011) analysed the CSR reports of 84 Fortune 100 organisations).

Sampling Criteria

The Fortune 100 Index of companies is used to select the sample as it has been used to empirically explore both privacy (e.g., Ashworth and Free, 2006) and the nonmarket environment (e.g., Martin et al., 2018). The Fortune 100 is a list of the top 100 organisations in the United States. It is a subset of the Fortune 500 listing, a list of 500 of the largest U.S. public and privately held companies, published by Fortune magazine. Fortune creates the list by ranking public and private companies that report annual revenue figures to a government agency, based on total revenues for the organisation's corresponding fiscal year (Kenton, 2021). The Fortune 100 list does not include foreign companies, although most of the listed companies have significant international operations. Due to their size, these organisations are also most likely to have published CSR reports, and to publish them in English.

This research uses the Fortune 100 listing from 2018, as the research was undertaken at the beginning of 2020 and the 2018 listing was the most recent at the time. Three companies in the Fortune 100 listing had since been acquired/merged i.e., Andeavor had been acquired by Marathon Petroleum, Direct TV had been acquired by AT&T, and 21st Century Fox had been acquired by Walt Disney. This meant 97 organisations were included in the final sample.

Sample Overview

To provide additional insight into the organisations, data from the Fortune 100 list were augmented with information from five additional sources; (i) the Fortune 500 financials, (ii) the Fortune 500 industry sector, (iii) the organisations' websites, (iv) the Forbes 'Just 100' index (Forbes, 2020), and (v) the Privacy Rights Clearinghouse (PRC) database (Privacy Rights Clearinghouse, 2021).

First, for each organisation, financial metadata i.e., employee numbers, revenue, profit, assets and market value, were downloaded from the Fortune 500 website[4]. For each organisation, the most recent financial valuations (2020) were selected, and the descriptive metadata for each organisation recorded. Second, the industry sector was also recorded. The industry sectors are those used in the Fortune 500 index, namely Chemicals, Energy, Financials, Food and Drug Stores, Food, Beverages and Tobacco, Healthcare, Industrials, Media, Motor Vehicles and Parts, Oil and Gas Equipment, Retailing, Technology, Telecommunications, Transportation, Wholesalers. The Finance sector accounts for 20% of the total sample, Healthcare accounts for 13.5% and four industries (Healthcare, Finance, Technology and Energy) account for 55% of the sample of reports. A breakdown of organisations by industry is included in Appendix H.

Third, the organisation's primary sales model (B2C = Business to Customer, or B2B = Business to Business) was also determined from their website details. In many cases, particularly in the technology sector, the organisations often reported both sales models. It seems reasonable to suggest that in the B2C model, more personal data will be collected and processed by the organisation, and therefore those organisations who were conducting B2C activities were considered more likely to be processing large amounts of consumer personal data. 43% were B2B only (*n=42*), 31% were B2C only (*n=30*) and 26% were both (*n=25*).

Fourth, the Forbes JUST-100 listing (Forbes, 2020) was searched to determine if any of the organisations in the Fortune 100 listing were referenced in the JUST-100 listing. The Forbes JUST-100, details the top 100 'Just' companies (from 928 of the largest publicly traded US organisations' data) and evaluates them based on their reported business activities in five key areas: treatment of workers, community, customers, shareholders and

[4]*https://fortune.com/fortune500/*

the environment, using public reports, surveys and crowdsourced repositories (Forbes, 2020). Where an organisation in the Fortune 100 listing was found to be ranked in the Forbes JUST-100, the rank was recorded in Table 5.2. 42% of the organisations in the sample used in this study (*n=41*) were ranked in the Forbes JUST-100. See Appendix J for a list of the organisations that appear in both listings. From our sample, 28.5% of organisations from the financial industry *(n=6*) and 47% of organisations from the Healthcare industry (*n=7*) were ranked in the Forbes JUST-100. 62.5% of organisations from the 'retailing' industry (*n=5)* and 60% of organisations from the Transport industry *(n=3)* were ranked in the Forbes JUST-100. Finally, 75% of organisations from the Telecommunications industry *(n=3*) and 80% of organisations from the Technology industry (*n=8)* were ranked in the Forbes JUST-100. Facebook was not ranked in the Forbes JUST-100, and neither was Oracle.

Finally, the number of breaches associated with the organisations are included, as reported in the privacyrights.org dataset (Privacy Rights Clearinghouse, 2021). This dataset includes over 5000 data breaches disclosed by firms, non-profit organisations, healthcare organisations and government agencies in the US, from 2005 to present. 36% the 97 organisations in the sample *(n=35)* reported data breaches. 40% of Healthcare organisations (*n=6*) reported a data breach, 27% of Finance organisations (*n=6)* reported a data breach, 30% of Technology organisations (*n=3*) reported a data breach, and 65% of Telecommunications organisations (*n=2*) reported a data breach.

An overview of the sample is presented in Table 4.7, in terms of financial details and industry classification, together with details on their CSR reports, their business models, rankings in the Forbes 100 Just Index where applicable, and reported data breaches from the PRC database, where applicable.

Table 4.7 CSR Reports Sample Overview

	Organisation	Industry	Business Model	Forbes JUST 100 Rank	Fortune Company Details					CSR Report			Data Breach
					Emps	Revenue $M	Profit $M	Assets $M	Market Value $M	Report ?	Incl Priv ?	Year	
1	**3M**	Chemicals	B2B	JUST 90	96,163	32,136	4,570.0	44,659	78,529	Yes	Yes	2020	-
2	**Aetna**	Healthcare	B2C	-	49,500	63,155	2,271.0	69,146	44,859	Yes	Yes	2019	-
3	**AIG**	Financials (insurance)	B2B, B2C	-	46,000	49,746	3,348.0	525,064	20,886	Yes	Yes	2019	-
4	**Allstate**	Financials (banking)	B2C	-	46,035	44,675	4,847.0	119,950	29,071	Yes	Yes	2019	-
5	**Alphabet**	Technology	B2B, B2C	JUST 5	118,899	161,857	34,343.0	275,909	798,905	Yes	Yes	2019	-
6	**Amazon**	Retailing	B2B, B2C	JUST 66	798,000	280,522	11,588.0	225,248	970,680	Yes	Yes	2020	1
7	**American Airlines Group**	Transportation	B2C	-	133,700	45,768	1,686.0	59,995	5,194	Yes	Yes	2018	-
8	**American Express**	Financials (banking)	B2C	JUST 89	64,500	47,020	6,759.0	198,321	68,983	Yes	Yes	2019	3
9	**Amerisource Bergen**	Healthcare (wholesale)	B2B	-	21,500	179,589	855.4	39,172	18,221	Yes	Yes	2019	-
10	**Anthem**	Healthcare (retail)	B2B, B2C	JUST 14	70,600	104,213	4,807.0	77,453	57,245	Yes	Yes	2018	2
11	**Apple**	Technology	B2B, B2C	JUST 3	137,000	260,174	55,256.0	338,516	1,112,641	Yes	Yes	2019	4
12	**Archer Daniels Midland**	Food, Beverages & Tobacco	B2B	-	38,100	64,656	1,379.0	43,997	19,603	Yes	No	2018	-
13	**AT&T**	Telecommunications	B2B, B2C	JUST 8	247,800	181,193	13,903.0	551,669	209,388	Yes	Yes	2019	9
14	**Bank of America**	Financials (banking)	B2C	JUST 12	208,131	113,589	27,430.0	2,434,079	185,227	Yes	Yes	2018	10
15	**Berkshire Hathaway**	Financials (holding)	B2B	-	391,500	254,616	81,417.0	817,729	442,897	Yes	No	2018	-
16	**Best Buy**	Retailing	B2C	JUST 25	125,000	43,638	1,541.0	15,591	14,647	Yes	Yes	2019	2
17	**Boeing**	Aerospace & Defence	B2B	-	161,100	76,559	-636.0	133,625	84,149	Yes	Yes	2019	5
18	**Cardinal Health**	Healthcare (distribution)	B2B	-	49,500	145,534	1,363.0	40,963	13,988	Yes	Yes	2019	1
19	**Caterpillar**	Industrials	B2B	-	102,300	53,800	6,093.0	78,453	63,832	Yes	No	2019	-
20	**Chevron**	Energy	B2B	JUST 61	48,200	146,516	2,924.0	237,428	136,176	Yes	Yes	2019	1
21	**CHS**	Food, Beverages & Tobacco	B2B	-	10,703	31,901	829.9	16,448	-	Yes	No	2020	-

	Organisation	Industry	Business Model	Forbes JUST 100 Rank	Fortune Company Details					CSR Report			Data Breach
					Emps	Revenue $M	Profit $M	Assets $M	Market Value $M	Report ?	Incl Priv ?	Year	
22	**Cigna**	Healthcare (insurance)	B2B, B2C	JUST 17	73,700	153,566	5,104.0	155,774	65,897	Yes	Yes	2019	2
23	**Cisco Systems**	Technology	B2B, B2C	JUST 9	75,900	51,904	11,621.0	97,793	166,709	Yes	Yes	2019	-
24	**Citigroup**	Financials (banking)	B2C	JUST 31	200,000	103,449	19,401.0	1,951,158	88,377	Yes	Yes	2019	4
25	**Coca-Cola**	Food, Beverages & Tobacco	B2B	JUST 95	86,200	37,266	8,920.0	86,381	189,983	Yes	No	2019	-
26	**Comcast**	Telecommunications	B2B, B2C	JUST 49	190,000	108,942	13,057.0	263,414	156,533	Yes	No	2020	3
27	**Conoco Phillips**	Energy	B2B	-	10,400	36,670	7,189.0	70,514	33,167	Yes	Yes	2019	-
28	**Costco Wholesale**	Retailing	B2B, B2C	-	201,500	152,703	3,659.0	45,400	125,908	Yes	No	2019	-
29	**CVS Health**	Healthcare (retail)	B2C	JUST 84	290,000	256,776	6,634.0	222,449	77,376	Yes	Yes	2019	5
30	**Deere**	Industrials	B2B	JUST 70	73,489	39,258	3,253.0	73,011	43,330	Yes	Yes	2019	-
31	**Dell**	Technology	B2B, B2C	JUST 35	165,000	92,154	4,616.0	118,861	29,246	Yes	Yes	2019	-
32	**Delta Air Lines**	Transportation	B2C	JUST 97	91,224	47,007	4,767.0	64,532	18,262	Yes	Yes	2019	-
33	**Dow**	Chemicals	B2B	-	36,500	42,951	-1,359.0	60,524	21,716	Yes	No	2019	-
34	**Dupont**	Chemicals	B2B	-	35,000	21,512	498.0	69,396	25,213	Yes	Yes	2020	-
35	**Energy Transfer**	Energy	B2B	-	12,812	54,213	3,592.0	98,880	12,374	Yes	No	2018	-
36	**Enterprise Products**	Oil & Gas Equipment	B2B	-	7,300	32,789	4,591.3	61,733	38,472	Yes	Yes	2019	-
37	**Express Scripts**	Healthcare (drug dispense)	B2C	-	25,600	100,288	3,404.4	51,745	39,567	No	No	No	-
38	**Exxon Mobil**	Energy	B2B	-	74,900	264,938	14,340.0	362,597	160,696	Yes	No	2018	-
39	**Facebook**	Technology	B2B, B2C	-	44,942	70,697	18,485.0	133,376	475,455	No	No	No	3
40	**Fannie Mae**	Financials (mortgages)	B2C	-	7,500	120,304	14,160.0	3,503,319	1,841	Yes	No	2018	-
41	**FedEx**	Transportation	B2B, B2C	JUST 82	389,500	69,693	540.0	54,403	31,679	Yes	Yes	2020	2
42	**Ford Motor**	Motor Vehicles & Parts	B2B	JUST 37	190,000	155,900	47.0	258,537	19,151	Yes	Yes	2020	-
43	**Freddie Mac**	Financials (banking)	B2C	-	6,892	75,125	7,214.0	2,203,623	909	No	No	No	-
44	**General Dynamics**	Aerospace & Defence	B2B	-	102,900	39,350	3,484.0	48,841	38,398	Yes	Yes	2018	-

	Organisation	Industry	Business Model	Forbes JUST 100 Rank	Fortune Company Details					CSR Report			Data Breach
					Emps	Revenue $M	Profit $M	Assets $M	Market Value $M	Report ?	Incl Priv ?	Year	
45	**General Electric**	Industrials	B2B	-	205,000	95,214	-4,979.0	266,048	69,406	Yes	Yes	2019	1
46	**General Motors**	Motor Vehicles & Parts	B2B	JUST 28	164,000	137,237	6,732.0	228,037	29,695	Yes	Yes	2019	1
47	**Goldman Sachs**	Financials (banking)	B2C	-	38,300	53,922	8,466.0	992,968	55,417	Yes	Yes	2019	-
48	**Halliburton**	Oil and Gas Equipmnt	B2B	-	55,000	22,408	-1,131.0	25,377	6,027	Yes	No	2019	-
49	**HCA Healthcare**	Healthcare (hospitals)	B2C	-	245,000	51,336	3,505.0	45,058	30,411	Yes	No	2019	-
50	**Home Depot**	Retailing	B2C	JUST 84	415,700	110,225	11,242.0	51,236	200,665	Yes	Yes	2019	4
51	**Honeywell**	Industrials	B2B	-	113,000	36,709	6,143.0	58,679	94,628	Yes	Yes	2020	2
52	**HP**	Technology	B2B, B2C	JUST 16	56,000	58,756	3,152.0	33,467	24,821	Yes	Yes	2019	-
53	**Humana**	Healthcare (insurance)	B2C	JUST 52	46,000	64,888	2,707.0	29,074	41,490	Yes	Yes	2019	4
54	**IBM**	Technology	B2B, B2C	JUST 11	383,800	77,147	9,431.0	152,186	98,551	Yes	Yes	2019	2
55	**Ingram Micro**	Wholesalers (books)	B2B	-	21,700	46,487	267.0	4,166	3,925	Yes	Yes	2018	-
56	**Intel**	Technology	B2B	JUST 4	110,800	71,965	21,048.0	136,524	231,662	Yes	Yes	2019	-
57	**Johnson & Johnson**	Healthcare (wholesale)	B2B	JUST 45	132,200	82,059	15,119.0	157,728	345,705	Yes	Yes	2019	-
58	**JPMorgan Chase**	Financials (banking)	B2C	JUST 6	256,981	142,422	36,431.0	2,687,379	276,750	Yes	No	2019	2
59	**Kroger**	Food & Drug Stores (retail)	B2C	-	435,000	122,286	1,659.0	45,256	24,114	Yes	Yes	2020	-
60	**Liberty Mutual**	Financials	B2C	-	45,000	43,228	1,044.0	133,644	-	Yes	Yes	2019	-
61	**Lockheed Martin**	Aerospace & Defence	B2B	JUST 53	110,000	59,812	6,230.0	47,528	95,539	Yes	Yes	2019	2
62	**Lowe's**	Retailing	B2C	-	260,000	72,148	4,281.0	39,471	64,963	Yes	Yes	2019	1
63	**Macy /Sears**	Retailing	B2C	-	140,000	22,138	-2,221.0	9,362	1,231	Yes	Yes	2018	-
64	**Marathon**	Energy	B2B	JUST 79	60,910	124,813	2,637.0	98,556	15,353	Yes	Yes	2019	-
65	**Mass Mutual**	Financials (insurance)	B2B, B2C	-	9,896	37,253	3,700.7	290,731	-	Yes	No	2019	-
66	**McKesson**	Healthcare (hospitals)	B2B	-	70,000	214,319	34.0	59,672	21,845	Yes	No	2019	-
67	**Merck**	Healthcare (drugs)	B2B	JUST 30	71,000	46,840	9,843.0	84,397	195,141	Yes	Yes	2019	-

	Organisation	Industry	Business Model	Forbes JUST 100 Rank	Fortune Company Details					CSR Report			Data Breach
					Emps	Revenue $M	Profit $M	Assets $M	Market Value $M	Report ?	Incl Priv ?	Year	
68	**MetLife**	Financials (insurance)	B2C	JUST 75	49,000	69,620	5,899.0	740,463	27,997	Yes	Yes	2018	1
69	**Microsoft**	Technology	B2B, B2C	JUST 1	144,000	125,843	39,240.0	286,556	1,199,550	Yes	Yes	2019	1
70	**Mondelez**	Food, Beverages & Tobacco	B2B	-	80,000	25,868	3,870.0	64,549	71,762	No	No	No	-
71	**Morgan Stanley**	Financials (investment)	B2B, B2C	-	60,431	53,823	9,042.0	895,429	52,102	Yes	Yes	2019	1
72	**Nationwide**	Financials (banking)	B2C	-	28,114	43,982	829.7	239,540	-	Yes	Yes	2019	-
73	**New York life**	Financials (insurance)	B2B, B2C	-	11,519	44,117	1,004.0	333,806	-	No	No	No	-
74	**Oracle**	Technology	B2B, B2C	-	136,000	39,506	11,083.0	108,709	152,413	Yes	Yes	2019	-
75	**PepsiCo**	Food, Beverages & Tobacco	B2B	JUST 24	267,000	67,161	7,314.0	78,547	166,848	Yes	No	2019	-
76	**Pfizer**	Healthcare (drugs)	B2B	-	88,300	51,750	16,273.0	167,489	181,075	Yes	Yes	2019	4
77	**Phillips 66**	Energy	B2B	-	14,500	109,559	3,076.0	58,720	23,490	Yes	No	2020	-
78	**Plains GP Holdings**	Energy	B2B	-	5,000	33,669	331.0	29,969	1,022	Yes	No	2019	-
79	**Procter & Gamble**	Healthcare (wholesale)	B2B	JUST 18	97,000	67,684	3,897.0	115,095	271,640	Yes	Yes	2019	-
80	**Prudential**	Financials (insurance)	B2B, B2C	-	51,511	64,807	4,186.0	896,552	20,650	Yes	Yes	2019	1
81	**State Farm**	Financials (insurance)	B2B, B2C	-	57,672	79,395	5,592.7	294,823	-	No	No	No	4
82	**StoneX Group**	Financials (investments)	B2B	-	2,012	32,897	85.1	9,936	700	No	No	No	-
83	**Sysco**	Wholesalers (food)	B2B	-	69,000	60,114	1,674.3	17,967	23,203	Yes	No	2019	-
84	**Target**	Retailing	B2C	JUST 15	368,000	78,112	3,281.0	42,779	46,574	Yes	Yes	2019	-
85	**Tech Data**	Wholesalers	B2B	-	15,000	36,998	374.5	13,269	4,645	Yes	Yes	2020	-
86	**TIAA**	Financials (insurance)	B2C	-	16,533	40,454	2,460.1	615,042	-	Yes	Yes	2019	-
87	**Tyson Foods**	Food, Beverages & Tobacco	B2B	-	141,000	42,405	2,022.0	33,097	21,125	Yes	No	2019	-
88	**United Airlines**	Transportation	B2C	-	96,000	43,259	3,009.0	52,611	7,823	Yes	No	2019	1
89	**UPS**	Transportation	B2B, B2C	JUST 39	377,640	74,094	4,440.0	57,857	80,196	Yes	Yes	2019	-
90	**United Health**	Healthcare (insurance)	B2C	-	325,000	242,155	13,839.0	173,889	236,555	Yes	Yes	2019	1

	Organisation	Industry	Business Model	Forbes JUST 100 Rank	Fortune Company Details					CSR Report			Data Breach
					Emps	Revenue $M	Profit $M	Assets $M	Market Value $M	Report ?	Incl Priv ?	Year	
91	**Valero Energy**	Energy	B2B	-	10,222	102,729	2,422.0	53,864	18,532	Yes	Yes	2019	-
92	**Verizon**	Telecommunications	B2B, B2C	JUST 42	135,000	131,868	19,265.0	291,727	222,220	Yes	Yes	2019	1
93	**Walgreens Boots**	Food & Drug Stores	B2C	-	287,000	136,866	3,982.0	67,598	40,528	Yes	No	2019	-
94	**Walmart**	Retailing	B2C	JUST 50	2,200,000	523,964	14,881.0	236,495	321,803	Yes	Yes	2019	-
95	**Walt Disney**	Media	B2B, B2C	-	223,000	69,570	11,054.0	193,984	174,405	Yes	Yes	2019	-
96	**Wells Fargo**	Financials (banking)	B2C	JUST 72	259,800	103,915	19,549.0	1,927,555	117,366	Yes	Yes	2019	-
97	**World Fuel**	Energy	B2B	-	5,500	36,819	178.9	5,992	1,647	Yes	Yes	2019	-

4.6.2 Design and Data Collection

First presented is an outline of the Online Delphi Survey method design and data collection, and this is followed by an outline of the collection of the CSR Reports.

4.6.2.1 Online Delphi Survey Design and Data Collection

The Delphi method is characterised by involving a panel of experts, without concern for geography, to reply anonymously to a number of iterative "rounds" of specific questions (Linstone and Turoff, 2002) in order to achieve group consensus. Understanding a phenomenon such as the amount of control or justice demonstrated by a given NMPv activity, is likely to be significantly influenced by expertise, experience, or occupational position of a participant (Linstone and Turoff, 2002). Therefore, there is a significant benefit in being able to harness subjective and anonymous judgements of multiple experts. Due to the geographically dispersed panel, and a need to complete in a reasonable timeframe, an Online Delphi Survey method was adopted in this research. The Online Delphi Survey method, sometimes referred to as an E-Delphi, provided numerous advantages over traditional approaches to the Delphi, including high quality data collection, ease and speed of survey administration, direct communication with the panel and rapid collation of feedback allowing data collection to be undertaken in a short time frame (Hasson et al., 2000). The following sections outline the design of the Online Delphi Survey method, under two key headings; the Online Delphi Survey method rationale, and the Online Delphi Survey method process.

The Online Delphi Survey Method Rationale

Any Delphi method is only appropriate to investigate certain research problems, so careful consideration must be given to the nature of the problem before selecting this approach (Hasson et al., 2000). Linstone and Turoff (1975) outlined four research objectives that call for the use of a Delphi method, namely (i) to explore or expose underlying assumptions or

information leading to differing judgements, (ii) to seek out information which may generate a consensus on the part of the respondent group, (iii) to correlate informed judgements on a topic spanning a wide range of disciplines, and (iv) to educate the respondent group as to the diverse and interrelated aspects of the topic. Understanding the nature of the problem and the logistical considerations that arise from the topic need to be established before deciding upon its use. The Delphi method has been found to be particularly useful in situations where a problem can benefit from subjective judgements from multiple experts, or where ethical/social dilemmas dominate economic or technical ones (Hanafin and Brooks, 2007; Linstone and Turoff, 1975). NMPv met both these conditions.

The Online Delphi Survey method has also been used in previous IS studies for framework development (Skinner et al., 2015). Sharma et al. (2008) likewise use the method to derive a conceptual framework for analysing knowledge societies. Finally, the overall purpose of the Online Delphi Survey method was to establish the levels of control and justice signalled by different NMPv activities i.e., to weight them. An Online Delphi Survey was considered an effective tool to achieve this purpose as participatory approaches involving expert judgement have often been used for the determination of weights, with a view to express relative importance of the indicators from a societal viewpoint (Saisana and Tarantola, 2002).

The Online Delphi Survey Method Process

The essence of the Online Delphi Survey method is multiple rounds of structured e-surveys, distributed to a panel of experts to verify hypotheses, identify key indicators, or rate importance of certain factors for a given issue (Skulimowski, 2017). The Online Delphi Survey method consists of two components; a panel of experts (referred to in this thesis as panelists) and a survey (Skulmowski et al., 2007). In the first round, the Online

Delphi Survey method traditionally begins with an open-ended survey which serves as the cornerstone of soliciting specific information about a content area from the panelists (Hsu and Sandford, 2007). However, it is a common modification to use a structured survey in the first round that is based upon an extensive review of the literature (Hsu and Sandford, 2007), or based on qualitative data already collected through focus groups/interviews (Lynn et al., 1998). This is referred to as a modified Delphi. The use of a modified Delphi method is appropriate if basic information concerning the target issue is available and usable (Kerlinger, 1973). Having already established a possible range of NMPv activities, a modified Online Delphi Survey method was conducted, where the first round contained both structured and unstructured questions.

The first step therefore was to define a comprehensive range of NMPv activities undertaken by organisations which were elicited from the extant literature on privacy and the nonmarket environment literature. The next step was to define the criteria for inclusion on the expert panel. Following this, two rounds of enquiry were presented to the panelists, followed by analysis/consensus. Thus, in the final stage of the Online Delphi Survey, the initial range of NMPv activities were validated and weighted. Figure 4.3 illustrates the research process.

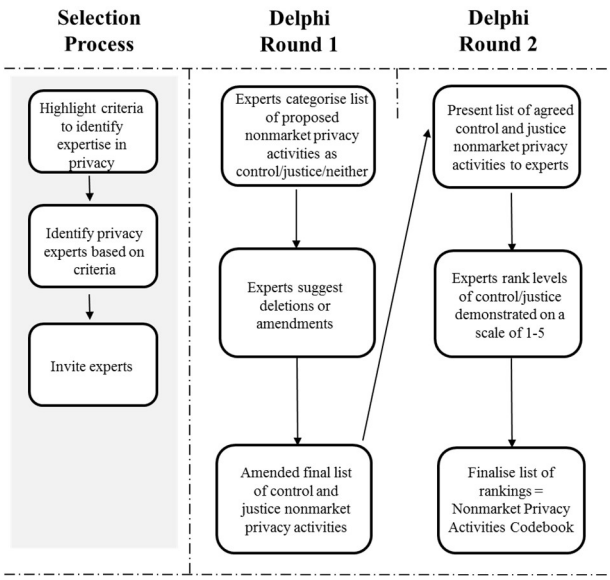


Figure 4.3 Online Delphi Survey Study Visualisation

In round one, the panelists were sent a survey via email, which was administered using Qualtrics. In this survey, the panelists were first presented with a narrative outlining privacy in the market environment and the nonmarket environment. This was followed by a brief summary of privacy as control or justice. A copy of the invitation, the survey instructions and narrative, and the surveys, are included in Appendix B, C and D respectively. The panelists were provided with a list (*n=40*) describing possible NMPv activities/properties referenced in previous studies (including Allen and Peloza, 2015; Culnan and Williams, 2009; Greenaway and Chan, 2013; Greenaway et al., 2015; Martin, 2016; Pollach, 2011).

Franklin and Hart (2006) emphasise the difficulty in creating the first Online Delphi Survey in this way, i.e., the risk of neglecting major issues due either to the fact they are recent and therefore not yet included in the literature or to the lack of recognition in the literature. Consequently, the panelists were asked to not only categorise the list provided as control or justice (or neither), but also to provide feedback if elements of NMPv not included in the list should be included, or if one listed should not be included. Reminder emails were sent after a week had elapsed. See Appendix E for a copy of the reminder emails. When all panelists completed this round, ambiguous privacy activities/properties and those without consensus, were removed from the list and adjustments made in line with panelist feedback.

In round two, a weighting system was required that would position NMPv activities on a control scale or a justice scale (low to high). This is because an organisation's approach to nonmarket privacy will not simply signal a binary measurement of control or justice, as organisations reflect varying levels of both, and always need to exercise a certain level of control over information in order to comply with legislation. Thus, in round two, the panelists were sent a survey outlining a list of NMPv activities, now categorised as either control or justice. The panelists were then tasked with weighting levels of control or justice

signalled by the NMPv activities appearing on the revised list, on a scale of 1-5, where 1 is low, and 5 is high. When completed, the second round contributed to the formation of the Nonmarket Privacy Activities Codebook.

It is important to note that although the items in the Nonmarket Privacy Activities Codebook are parsimoniously referred to in the remainder of this thesis as 'NMPv activities', the researcher accepts that they are both privacy activities and organisational properties/characteristics.

4.6.2.2 CSR Reports Data Collection

Saunders et al. (2007) created three subgroups of secondary data, namely documentary data, survey-based data and multiple data. Documentary data include written materials such as journals, newspapers, books, publications, reports to shareholders, diaries, minutes of meetings, notices and correspondence. In Study One, CSR reports are used as a source of secondary data. The following sections outline the collection of the CSR reports, under two key headings, namely; the rationale for selecting CSR reports as a source of data, and the CSR reports collection process.

CSR Reports Rationale

The advantages of secondary data sources include the extensive span of data availability and the quality of professionalism and expertise involved (Pérez-Sindín, 2017). The major drawback of this source is the non-involvement of the researcher in the collection process (Saunders et al., 2007). A CSR report is an auditable, internal and external facing document that organisations use to communicate CSR efforts and their impact on the environment and community (Cote, 2021; Kolk, 2003). CSR reports have been used as a secondary data source in previous nonmarket environment and privacy studies e.g., Fuoli (2018), Johnson et al. (2011), Nwagbara and Belal (2019) and Pollach (2011). 90% of the largest 500 global companies publish CSR reports in 2019 (Cote, 2021; Governance and

Accountability Institute, 2020). CSR reports typically signal what an organisation perceives as important, whereas less important items are absent or relegated (Gibson and Guthrie, 1996). Furthermore, what organisations choose to include or omit from their corporate reports reflects a significant message to stakeholders.

CSR Reports Collection Process

As previously noted, three companies in the Fortune 100 listing had since been acquired/merged, which meant ninety-seven organisations were included in the sample. For each of the ninety-seven organisations in the sample, the CSR section on their website was accessed to source an official CSR report. Whether an organisation publishes a CSR in printable form e.g., a PDF, or an interactive online form e.g., website section – for simplicity both are referred to as a CSR Report in this thesis. Terminology used to describe CSR reports varied (for example, global sustainability reports, social responsibility publications, and corporate social responsibility reports) so each search included multiple terms. Where such a report could not be found, the CSR section, on the organisation's website (if any) was copied into a word document. Ninety organisations were found to publish some form of CSR report, and seven organisations found to not publish any form of CSR report. For the organisations who published some form of CSR report, their documents were then imported into NVivo (V12). CSR reports are typically produced in the current year, for the previous annual or bi-annual period, therefore the majority of our sample of CSR data fell between 2018-2020.

Europeans interpretation of the term 'data protection' and 'privacy' differs to that of Americans (SANS, 2018). For instance, US legislation uses the term 'California **Consumer Privacy** Act', where for a similar act, European legislation uses the term General **Data Protection** Regulation'. To determine if there were any NMPv activities reported in the ninety CSR publications, the reports were first searched using the following keywords: 'privacy' and 'data protection'. They were also searched using the terms

'cybersecurity' and 'governance', as these terms often contained references to encryption and other privacy enhancing tools. Almost a quarter of the organisations who published some form of CSR report, did not frame privacy as a nonmarket activity (*n=25*), where the remainder did (*n=65*). Interestingly, all the organisations in the 'Food and Beverages' industry i.e., Archer Daniels, CHS, Coca-Cola, Mondelez, PepsiCo and Tyson Foods, did not frame privacy as a NMPv activity in their CSR reports.

4.6.3 Data Strategy

This section first describes the data analysis for the Online Delphi Survey and then the data analysis for the CSR Reports.

4.6.3.1 Online Delphi Survey Data Strategy

Skinner et al. (2015) advocate that when reporting any Delphi method analysis, a number of details should be included. Table 4.8 outlines these details together with how they are considered in this study.

Table 4.8 Online Delphi Survey Details (as advocated by Skinner et al., 2015)

Detail recommended by Skinner at al., (2015)	Detail in this Study
Study purpose	To establish/validate list of NMPv activities that will form a coding framework to be used for a larger study involving thematic analysis.
Duration	Four weeks.
Number of rounds	Two.
Number of issues	Forty in round 1. Two NMPv activities removed, two NMPv activities added. Forty in round 2.
Number of panels	One.
Participation rate	Seventeen experts invited. Fourteen agreed to participate.
Sample size per round	Fourteen in round one. Twelve in round two.
Delphi design type	Modified Online Delphi Survey (Linstone and Turoff, 2002).
Questionnaire design	Exploratory.
Panel selection procedure	At least two of five explicit expert criteria.
Consensus approach	Round 1: Fifty-one % or more. Round 2: Median.

The Online Delphi Survey method adopts the data analysis techniques of the traditional Delphi method. Data analysis can involve both qualitative and quantitative data (Hsu and Sandford, 2007), requiring both statistical and consensus analysis. The major statistics used in most Delphi studies are measures of central tendency (means, median, and mode) and level of dispersion (standard deviation and inter-quartile range) in order to present information concerning the collective judgments of respondents (Hasson et al., 2000). The use of median score, based on Likert-type scale, is strongly favoured in the literature (Ab Latif et al., 2017; Hill and Fowles, 1975; Jacobs, 1996). The use of mode is also suitable when reporting data in the Delphi process (Ab Latif et al., 2017; Ludwig, 1994). In some cases, the mean is also workable (Murray and Jarman, 1987). However, the appropriateness of using the mean to measure the subjects' responses, if scales used in Delphi studies are not delineated at equal intervals, is considered questionable (Witkin, 1984; Hsu and Sandford, 2007). In line with Toma and Picioreanu (2016), the median is used in this Online Delphi Survey as a measure of central tendency, and frequency tables for the distribution of answers. These choices are justified by the ordinal nature of the variable, as a discrete variable with ordered categories (Kampen and Swyngedouw, 2000). This indicates an order of the more than/less than type, but it does not show the magnitude of the difference between the choices of answer (Kampen and Swyngedouw, 2000).

Decision rules need to be established to assemble and organise the judgments and insights provided by the Delphi panelists, however the kind and type of criteria to use to both define and determine consensus in any type of Delphi study is subject to interpretation (Hsu and Sandford, 2007). The consensus definition used commonly is the percentage of agreement based on a predefined cut-off, central tendency, or a combination of both. Consensus on a topic can be decided if a certain percentage of the responses fall within a prescribed range (Miller, 2006). However, percentage agreement varies widely e.g., 50%-97% (Nasa et al., 2021), or 20% -100% (Niederberger and Spranger, 2020), or 51%-80%

(von der Gracht, 2012). A universally agreed proportion does not exist for the Delphi method, as the level used depends upon sample numbers, aim of the research and resources. Keeney et al. (2007) suggest that the answer to the consensus debate may lie with the importance of the research topic. For instance, if it were a life and death issue such as whether or not to switch off a respirator, they suggest a 100% consensus level may be desirable. Alternatively, if the topic was related to a less impactful subject, a consensus of 51% may be acceptable (Keeney et al., 2007). Loughlin and Moore (1979) suggest that consensus should be equated with 51% agreement amongst respondents. McKenna (1994), drawing on Loughlin and Moore's work (1979), also suggests that consensus should be equated with 51% agreement amongst respondents. More recently Giannarou and Zervas (2014) also used a consensus cut-off of 51%. Thus, in this study consensus was considered to be achieved after 51% in the first round. Notably, most responses achieved more than 60% consensus. In the second round, the median was calculated for the weightings. Additional tests for stability and participation did not apply, because each round of the Online Delphi Survey has differing goals. The first round aims to establish whether a NMPv activity was a control activity or a justice activity, and the second round aims to weight the levels of control or justice each NMPv activity signals.

Round 1: This survey began with a narrative describing definitions of control and justice and definitions of NMPv activities, and was followed by a list of possible NMPv activities/properties. In the survey, the participants were asked to categorise the NMPv activities in the list as control/justice/neither, and to provide feedback if there were NMPv activities not included in the list that should be included, or if an NMPv activity listed should not be included. The responses were then analysed, and consensus calculated. Consensus was calculated by taking the number of majority opinions and dividing it by the number of total opinions (von der Gracht, 2012). After round one, two NMPv activities were removed from the list due to feedback. For instance ‘philanthropic cheque-book

privacy' was included in round 1, based on the 'philanthropic' pillar in Carroll's 1979 Pyramid of Responsibilities. However the researcher received comments from a journal editor during this period, that this was an old model of CSR and that more novel models of CSR had since been introduced that defined CSR differently. Comments received during the Online Delphi Survey, round one, also indicated that whilst in theory 'Chequebook Privacy' might exist – it didn't happen in reality. This NMPv activity was therefore removed. Feedback was also received that the NMPv activity 'aimed at stakeholder engagement' was very similar to 'aimed at internal/external stakeholder'. Therefore this NMPv activity was also removed.

The following section presents two examples from the responses to explain how the analysis was conducted. See below for an extract from the round 1 results – detailing the result for the NMPv activity: '*The organisation has appointed responsibility for privacy at C-Suite level'.*

Panelist:	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	Mdn	Control or Justice?	Consensus
C-Suite	2	2	1	1	3	2	2	3	2	1	2	2	2	2	2	Justice	64.29%

1' represents Control. '2' represents Justice, and '3' represents Neither.

Consensus was achieved at 51% agreement – as noted earlier in line with recommendations from McKenna (1994), Loughlin and Moore (1979) and Giannarou and Zervas (2014). In the above example there were 9 'justice' responses out of 14 possible responses, and this equated to 64.29%. In this way 64.29% of the panel of experts agreed that the appointment of a senior privacy executive, responsible for privacy, was a justice-based NMPv activity. This percentage exceeded the consensus threshold of 51% (McKenna, 1994), and therefore this NMPv activity was classified as a justice-based NMPv activity. In some cases *(n=9)* there was ambiguity i.e., no consensus could be achieved, or comments indicated ambiguity. In these cases, the comments from participants were reviewed, in order to determine if there was a reason for the ambiguity and to determine if the NMPv activity

needed to be removed or re-worded. For these ambiguous items, a consistent comment from participants was that "whilst there was a 'neither' option, there was no 'both' option". In other words, whilst the participants chose 'neither' they had wanted to choose 'both, and the survey design had not provided this option. See below for an extract from an ambiguous result for the NMPv activity '*The organisation participates in public debates regarding privacy'*.

Panelist:	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	Mdn	Control or Justice?	Comment
Participate Public-Debates	2	3	1	2	3	3	3	3	3	3	1	2	2	2	2.5	Neither	*Panelists called for a 'both' option*

1' represents Control. '2' represents Justice, and '3' represents Neither

After round one was completed, only two NMPv activities were removed and two NMPv activities were added, due to panel feedback. Nine ambiguous NMPv activities were incorporated into round two. For clarity, these ambiguous activities are marked with an * in Table 5.5.

Round 2: The panelists were first asked to weight the NMPv activities that received consensus in round one, in terms of how much control or justice they signalled, on a scale of 1-5, where 1 was low and 5 was high. The median was calculated for these weightings. Then ambiguous NMPv activities from round one were also presented to the panelists, in the second part of round 2. The panelists were asked if they agreed that these NMPv activities signalled 'neither' control nor justice or 'both' control and justice, and if they chose 'both' – they were asked if the NMPv activities signalled more justice than control, more control than justice, or equal levels of both. These NMPv activities were then assigned a weighting of 1 in their respective theme of control or justice, as they were deemed to express low levels of control or justice. Round 2 results formed the Nonmarket Privacy Activities Codebook, used as the codebook for the subsequent thematic analysis. The codebook included 15 control-based NMPv activities and 25 justice-based NMPv activities. See Table 4.9 for the control and justice totals from round 2.

Table 4.9 Final Results of the Online Delphi Survey

	Code Description	Weight (Delphi)	Code
	Control		
1	The organisation's privacy activities are aimed only at external stakeholders	1	Aim@ExternStake*
2	The organisation's privacy activities are aimed only at internal stakeholders	1	Aim@InternStake*
3	The organisation's privacy activities are driven by compliance	1	DrivnByComplnce*
4	The organisation has limited staff assigned to privacy activities	1	LimitfStaff4Priv*
5	The organisation appoints low profile non-exec privacy management	1	LowProfileNonExecs*
6	Limited budget is assigned to privacy activities	3	LimitedBudget4Priv
7	The organisation's stakeholders are not privacy aware	3	StakeNoPrivAware
8	The organisation is transaction-focused	3	TransFocused
9	The organisation does not publish values towards privacy in corporate publications	3.5	NoValuesPublished
10	The organisation lobbies governments for privacy standards that are most beneficial to the organisation	4	LobbyBenefitOrg
11	Ownership is shared between the individual and the organisation, where the organisation exercises more ownership	4	SharedOwnerOrgMore
12	The organisation's privacy behaviours are aimed at stockholder/share value	4	StockHolderShareValue
13	The organisation is data-focused	5	DataFocused
14	The organisation is inference-focused	5	InfererenceFocused
15	The organisation operates as information owner	5	InfoOwner
	Justice		
16	The organisation advises public policy on privacy	1	AdvisePublicPolicy*
17	The organisation associate's privacy with brand in corporate publications	1	PrivLink2Brand*
18	The organisation associates/funds privacy conferences	1	PrivLink2Conferences*
19	The organisation participates in public debates on privacy	1	PrivPublicDebate*
20	Ownership of personal information is shared, where the individual exercises more ownership	1	SharedOwnerIndividualMore
21	The organisation's privacy behaviours are driven by FIPPs	3.5	DrivnByFIPPS
22	The organisation's privacy behaviours are driven by stakeholder loyalty	3.5	DrivnByStakeLoyalty
23	The organisation appoints privacy representative to C-Suite	4.5	CsuiteExecAppoint

	Code Description	Weight (Delphi)	Code
24	The organisation's privacy behaviours are driven by stakeholder trust	4.5	DrivnByStakeTrust
25	Maximised budget is assigned to privacy activities	4	MaxBudget4priv
26	The organisation is advice-focused - aiming to build relationships with individuals	4	AdviceFocused
27	The organisation develops open standards for privacy	4	DevelopOpnStds
28	The organisation appoints privacy representative to management level	4	DPManagerAppoint
29	The organisation's privacy behaviours are driven by code of ethics	4	DrivenByCodeEthic
30	The organisation's privacy behaviours are driven by stakeholder respect	4	DrivnByStakeRespect
31	Privacy related employee training exceeds regulatory minimum	4	EmpTrainExceedsRegMin
32	The organisation operates as steward of information.	4	InfoSteward
33	The organisation lobbies for privacy standards most beneficial to the consumer	4	LobbyBenefitConsumer
34	Maximised staff assigned to privacy activities	4	MaxStaff4Priv
35	The organisation publishes values towards privacy in corporate publications	4	ValuesPublished
36	The organisation has strategic collaboration(s) with privacy advocacy groups	5	CollabAdvocacyGrps
37	The organisation exceeds privacy regulatory minimums	5	ExceedsRegMin
38	The organisation lobbies for privacy standards more beneficial to society	5	LobbyBenefitSociety
39	The organisation links privacy initiatives to stakeholders	5	PrivLink2Stakes
40	The organisation's stakeholders value privacy	5	StakesValuePriv

* *Ambiguous activities from round one that were presented again in round two*

4.6.3.2 CSR Report Data Strategy

The CSR reports were analysed using thematic analysis (Braun and Clarke, 2006), leveraging the matrix approach to thematic analysis (Groenland, 2018). Thematic analysis is a qualitative descriptive approach for identifying, analysing, and reporting themes/patterns within data (Braun and Clarke, 2020). Whilst many authors have maintained that thematic analysis is not a separate method, rather something to be used to assist researchers in analysis (Boyatzis, 1998; Holloway and Todres, 2003; Ryan and Bernard, 2000). Where other scholars argue it should be considered a method in its own right (Braun and Clarke, 2006; King, 2004; Leininger, 1992; Thorne, 2000). Thematic analysis is sometimes called Qualitative Content Analysis (Kuckartz, 2014) or Thematic Content Analysis (Vaismoradi et al., 2013), and is today one of the most commonly used methods for analysing qualitative data (Kuckartz and Radiker, 2019). Unlike traditional content analysis however, thematic analysis extends beyond counting words or pages in a set of texts and can explore explicit and implicit meanings within the data (Guest et al., 2012).

The use of the matrix approach enabled the researcher to demonstrate operability of the Nonmarket Privacy Activities Codebook to position an organisation's NMPv orientation, using 'tallies' of themes. In this way, a deductive approach to thematic analysis was conducted using a codebook, and the matrix approach was leveraged to produce the 'tallies' to position an organisation's NMPv orientation. The analysis of themes using the Nonmarket Privacy Activities Codebook was also used to provide additional insight into the NMPv activities currently being reported by some of the largest organisations in the US.

This section outlines the design of this stage, under two key headings, namely (i) the rationale for the selection of thematic analysis as a research approach, and (ii) an outline of the process of categorisation/coding conducted.

Rationale for Thematic Analysis

A rigorous thematic analysis can produce trustworthy and insightful findings (Braun and Clarke, 2019). Thematic analysis was selected for four key reasons. First, thematic analysis has frequently been used to analyse CSR publications in previous studies (e.g. Tate et al., 2010; Ozdoro-Aksak and Atakan-Duman, 2016). Second, thematic analysis is really useful for summarising key features of a large data set, as it forces the researcher to take a well-structured approach to handling data, helping to produce a clear and organised final report (King, 2004). Third, one of the hallmarks of thematic analysis is it's flexibility towards framing theory, research questions and research design (Braun and Clarke, 2006). Through this theoretical freedom, thematic analysis provides a highly flexible approach that can be modified for the needs of many studies, providing a rich and detailed, yet complex account of data (Braun and Clarke, 2020; King, 2004). Finally, as thematic analysis does not require the detailed theoretical and technological knowledge of other qualitative approaches, it offers a more accessible form of analysis.

The Process of Theme Categorisation

The terms category and theme are sometimes used interchangeably resulting in a lack of cohesion between the method of data analysis and the result (Vaismoridi et al., 2016). Therefore, at the beginning of the description of the theme development process, there is a need to describe the meaning of 'category' and differentiate it from 'theme', in terms of level of depth and abstraction.

The theme construction in this study is simplified to two key themes – a theme labelled 'Control' and a theme labelled 'Justice'. These themes could similarly have been called 'Power' and 'Responsibility', however given the use of the terms of control and justice in almost all privacy studies, control and justice were selected as the labels for the themes. The meaning of category is attributed by the researcher, and it may consist of

subcategories that identify the meaning of category (Constas, 1992). Category is the primary product of analytical process and has a descriptive identity. Researchers develop category at the beginning of the data analysis process to enter the abstraction process. Category development helps with the provision of details for analytical theme development. Constas (1992) presents a process for categorisation that consists of three components; (i) origination, (ii) verification, and (iii) nomination. A summary of details of each component is presented in Table 4.10.

Table 4.10 The Categorisation Process

Source (Constas, 1992)

Components	Description
Origination	• Using participant as a point of origination means that the participants can identify categories as opposed to a researcher identifying categories. • Using the investigator as a point of origination, categories are developed based on the personal interests, views or intellectual constructions of the researcher. • The researcher can refer to research or published works in the relevant area and derive categories from statements in that they are not directly related to the phenomena under investigation but are more related to the method of the analysis.
Verification	• Verification is used to support the creation and application of categories in a given study. • It consists of sources of external (utilizing a panel of experts outside of the study to verify and substantiate categories), rational (relying on relies on logic and reasoning, referential (utilizing existing research findings or theoretical arguments to justify categories), empirical (relying on internal data and without reference to other studies to examine the coverage and distinctiveness reflected by categories), technical (borrowing procedures, or at least language, from the quantitative orientation), and participative (providing participants the opportunity to review and possibly modify categories).
Nomination	• Concerned with naming categories. • The labels may be identical to those used under the origination component. • Participants can be a source of labelling. • Category names can be derived from existing theories and body of literature. • Labels can be derived from interpretative orientation.

Following the process of categorisation from Constas (1992) and in order to ensure an enhanced level of rigour in the coding scheme, the categories were firstly determined by the literature (the origination component) and were then validated and enhanced by the panelists (the verification component). This formed the Nonmarket Privacy Activities Codebook, which consisted of the themes of control or justice, and categories represented by NMPv activities associated with control or justice. The themes of control and justice

were input into Nvivo as nodes, and the categories were input as subnodes associated with their respective theme of either control or justice (the nomination component).

Each CSR report was then imported into NVivo as a data file and coded using this coding scheme. There was little interpretation of the coding by the researcher, as the search terms and coding frame were specific. The resulting thematic categories and subcategories were analysed by both (i) text and (i) frequency of occurrence in the dataset (e.g., Brough et al., 2009). Including frequency of occurrence enhances the qualitative analysis by generating descriptive statistics that allow for the identification of patterns in the data, which may have been missed through qualitative analysis alone (Collingridge, 2013). Quantitising the data in this way is achieved through 'counting' (Collingridge, 2013), where occurrences of categories and themes are counted. Using excel, the occurrence of each nonmarket activity was then weighted, by applying the weightings in the coding.

4.6.4 Quality Criteria

Quality in qualitative research remains 'a complex area' (Creswell, 1998, p. 193). There is considerable debate as to whether the principles of generalisability, validity, and reliability, which many consider to be deeply rooted within positivist research, can be applied to studies adopting a qualitative approach (Aguinis and Solarino, 2019; Healy and Perry, 2000). Researchers have argued that in qualitative research, new quality criteria terms such as credibility, transferability, and conformability better reflect the interpretivist outlook (Lincoln and Guba, 1985). Others have argued that quantitative principles can be applied but need to be modified to take account of the differing features and goals of qualitative research (Mays and Pope, 2000). Whilst the views of researchers such as Lincoln and Guba (1985) are acknowledged, the latter viewpoint is taken within this research. Thus, the concepts of generalisability, validity, and reliability within Study One are outlined below:

Generalisability: Although the generalisability of qualitative data is often questioned, findings should at least be made transferable to additional contexts (Venkatesh et al., 2013). Generalisation can be applied in a number of ways, such as generalising from one particular study context to another (Ritchie and Lewis, 2003). To enable this to occur, the provision of a 'thick description' (Geertz, 1973) of the original research process and setting needs to be provided. A clear demonstration that the sample is a true reflection of the population studied, and that the conclusions drawn are an accurate reflection of the data, is also important (Ritchie and Lewis, 2003).

Within the context of this study, the data collected in the Online Delphi Survey responses and CSR reports, were used to strengthen the interpretation provided. The use of the matrix approach to thematic analysis further facilitated the levels of interpretation. Furthermore, scrutiny was placed upon the way in which the research was conducted and designed to further explore any features of the research, such as the use of strict sampling criteria (the Fortune 100 index) for the CSR reports. CSR reports are considered legitimate and auditable documents often used to make stakeholders aware of the social and environmental activities and strategies conducted by companies (Kolk, 2003). CSR reports typically signal what an organisation perceives as important, whereas less important items are absent or relegated (Gibson and Guthrie, 1996).

Validity: is described as the extent to which a method measures what it is intended to measure. Threats to validity arise principally from pressures for convergence of predictions (Hill and Fowles, 1975), which undermines the Delphi's forecasting ability (Hasson et al., 2000). However, the use of panelists with subject matter expertise may help to increase the content validity, and the use of successive rounds of the questionnaire helps to increase the concurrent validity (Goodman, 1987). As previously mentioned, the Online Delphi Survey method is based upon the assumption that several people are less likely to arrive at a wrong

decision than a single individual. Decisions resulting from the Online Delphi Survey method are therefore strengthened by reasoned argument, thus helping to enhance validity.

Validity is also addressed with both face validity and content validity tests undertaken as part of the Online Delphi Survey method, controlling extraneous variables, and using standardised instructions. Face Validity is the subjective judgment that the survey measures what it intends to measure in terms of relevance and presentation (Babbie, 2001). The Online Delphi Survey was subject to a series of face validity tests undertaken by three DCU academic staff familiar with the technique. Feedback from the face validity tests were considered and the survey updated. Content Validity refers to the judgments of a panel of experts about the extent to which the content of the survey appears logically to examine and comprehensively include the characteristics of the domain being explored. Content validity can be achieved by (i) developing a data collection instrument that is informed by published literature, (ii) pretesting the instrument, (iii) carefully analysing the data from the first questionnaire and (iv) including expert panelists (Shariff, 2015). The content in the Online Delphi Survey is informed by both the NMPv activities reported in the literature and in the NMPv activities published in the sample of CSR reports. The iterative component was achieved in this study through two 'rounds' of a survey, and these rounds confirm the validity of the content by giving the expert panelists an opportunity to review the results of each round (Goodman, 1987).

Reliability: Closely corresponding to the notion of 'dependability' (Cypress, 2017), reliability is defined as the extent to which results are consistent over time and an accurate representation of the total population under study (Joppe, 2000). If the results of a study can be replicated under a similar methodology, then the research instrument is considered to be reliable (Joppe, 2000). To achieve reliability, researchers can ensure the research process is logical, traceable, and clearly documented (Tobin and Begley, 2004).

To enhance the reliability of the Nonmarket Privacy Activities Codebook, an Online Delphi Survey was conducted. The use of a codebook that was established and validated by the panelists, was selected over the use of multiple independent coders and inter-rater reliability measures, as there is much criticism over their use (e.g., Braun and Clarke, 2006; Braun and Clarke, 2020; Yardley, 2008). Morse (1997) for instance argues that such coding is superficial to facilitate coding agreement and both Braun and Clarke (2020) and Yardley (2008) argue that all coding agreement demonstrates is that coders have been trained to code in the same way not that coding is 'reliable' or 'accurate'. For those committed to qualitative research values, researcher subjectivity is viewed as a resource, rather than a threat to credibility, and so concerns about reliability do not hold (Braun and Clarke, 2006). In thematic analysis, the investigator is the instrument, and reliability among investigators is not typically assessed (Braun and Clarke, 2006). There is no one correct or accurate interpretation of data, as interpretations are inevitably subjective and reflect the positioning of the researcher (Braun and Clarke, 2021). In more recent thematic analysis studies, the subjectivity of the researcher is seen as integral to the process of analysis (e.g. Clarke et al., 2015, Braun, Clarke and Terry, 2014). In codebook thematic analysis, codebooks are not typically used to facilitate the measurement of intercoder agreement but are rather oriented to pragmatic considerations such as meeting predetermined information needs or a more efficient analysis (Braun and Clarke, 2021).

A structured approach to thematic analysis was followed, where coding reliability was achieved by iterative rounds involved in the Online Delphi Survey, and credibility achieved via the use of several privacy experts as proxy coders. Keeney et al. (2011) suggest that the Delphi method enhances reliability because (i) in the decision making process the panel members are anonymous to each other (thus eliminating group bias or group thinking), and (ii) the panel size and iterative rounds increase the reliability. The use of a codebook also provided a clear trail of evidence for Study One (Nowell et al., 2017).

For the CSR reports, reliability is achieved by using the organisation's own proprietary publications rather than third parties. CSR reports have been used in previous studies e.g., Fuoli (2018); Johnson et al. (2011); Nwagbara and Belal (2019).

4.7 Study Two

Study Two uses an Experimental Vignette Methodology (EVM). In an EVM study, participants are typically asked to imagine themselves in certain hypothetical scenarios i.e., short, carefully constructed scenarios describing a person, object, or situation, representing a systematic combination of characteristics (Atzmüller and Steiner, 2010). Participants are then presented with a survey, aimed at assessing dependent variables, such as their intentions, attitudes, and behaviours (Aguinis and Bradley, 2014).

Study Two involves two experiments. The first experiment sought to determine the influence of one NMPv activity, Corporate Political Privacy, on privacy concern, consumer trust, and purchase intention. Once the hypotheses were tested, and the hypothesised relationships confirmed, further exploration of different NMPv activities was required. Thus, the second experiment sought to determine the influence of different NMPv activities on privacy concern, consumer trust and continuance intention. Continuance intention was measured rather than purchase intention, as the experimental vignettes in the second experiment described a scenario that involved the continued use of an email system, rather than the purchase of a product or service. This section presents an outline of Study Two under five key headings, namely (i) sampling strategy, (ii) EVM design, (iii) survey design, (iv) data preparation and analysis, and (v) quality criteria. A visual summary of Study Two's research process is presented in Figure 4.4.

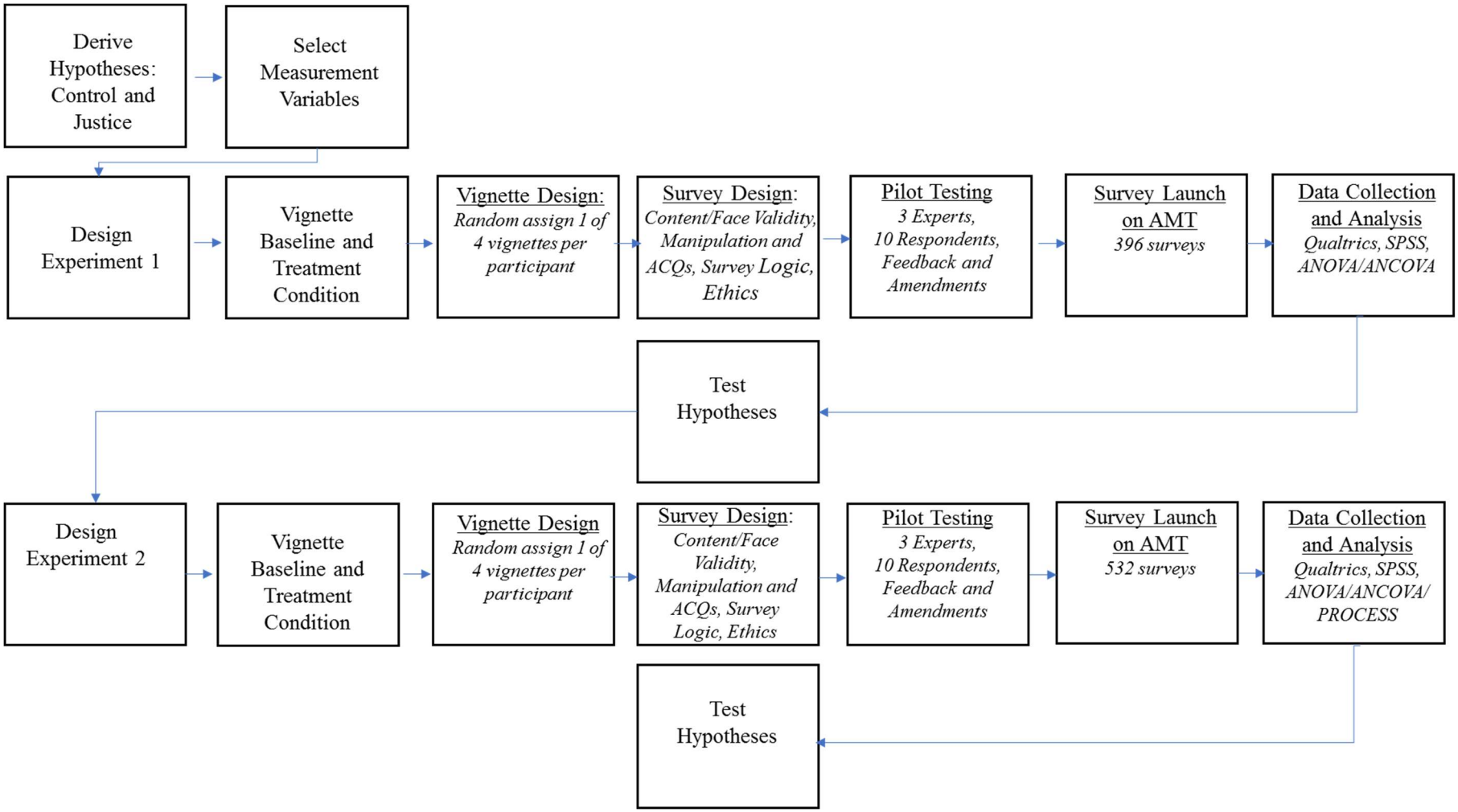


Figure 4.4 Study Two Research Process

4.7.1 Sampling Strategy

The remainder of this section discusses sampling strategy under four headings, namely sample size, participant recruitment and sample demographic.

4.7.1.1 Survey Population and Sampling

The target population for Study Two was US consumers. This population was selected for two reasons. First, face-validity tests were conducted by experts, which included US-based experts, and their feedback indicated some ambiguity between Europeans and Americans regarding the terms 'privacy' and 'data protection'. Europeans' interpretation of the term 'data protection' and 'privacy' differs to that of Americans (SANS, 2018). For instance, US legislation uses the term 'California Consumer **Privacy** Act', where for a similar act, European legislation uses the term General **Data Protection** Regulation'. Therefore it was decided to select either Americans OR Europeans. Second, the vignettes describe scenarios involving lobbying, which is a more open and transparent activity in the US than Europe, as the US requires systematic disclosure of lobbying, and is one of only a few countries to have such extensive requirements (Kerr et al., 2011). US consumers were thus selected as the target population. To reach the population, Study Two uses Amazon Mechanical Turk (AMT) workers who are registered in the US. Although the use of AMT for empirical research is debated (Barends and de Vries, 2019; Hydock, 2018; Zack et al., 2019), AMT was selected for several reasons. First, because its population has been found to be nationally representative (Gao and Milanaik, 2020; Martin, 2013). Second, it has previously been used in privacy studies (Martin, 2013; Martin, 2020; Martin and Nissenbaum, 2017). Third, AMT captures consumers most likely to be online (Tucker, 2014). Finally, AMT has been found to be a reliable source of respondents (Daly and Nataraajan, 2015).

Study Two uses convenience sampling. Convenience sampling is a type of non-probability or non-random sampling where members of the target population that meet certain practical criteria, such as easy accessibility, availability at a given time, or the willingness to participate, are included for the purpose of the study (Etikan et al., 2016). Convenience sampling methods place primary emphasis on generalisability i.e., ensuring that the knowledge gained is representative of the population from which the sample was drawn. Using a convenience sample allows researchers to purposefully select a panel of experts who can apply their knowledge to a specific issue/problem (Akins et al., 2005). This is particularly useful when there are only a limited number of experts in a field of interest, such as is the case with privacy.

4.7.1.2 Sample Size

Sample size is considered important because it impacts on the precision, reliability, and internal validity, and ultimately affects how confident we are that the sample results truly reflect population parameters (Cavana et al., 2001). Too small a sample size interacts with the power of the statistical tests to negatively impact upon the probability of achieving statistically significant results (Cohen, 1988).

Gray et al. (2017) note that for EVM, there are few prescriptions in terms of sample size. In a vignette study, some depth is traded for breadth of responses – meaning data needs to be collected from more participants than is traditional in, say, interview-based qualitative studies. The sample size is largely determined by EVM design. If there are lots of versions of a vignette, then more participants will be required to allow for enough data to make meaningful comparisons. Likewise, the more comparisons required between participant groups (for example, based on gender or age) then the more participants need to be recruited. For quantitative studies, sample size can be calculated using a power analysis from a chosen probability of finding a statistically significant result (power) for a given

population effect magnitude (Aberson, 2019; Brysbaert, 2019; Cohen, 1988). Using the G Power sample size rules (Erdfelder et al., 2007), with effect size f2 = 0.25, $\alpha = 0.05$, power = 0.95; this study required a total sample of 280 participants per experimental group. However based on the *post hoc* F test with a sample size of 390 participants per experiment, there was an increase in the power effect to $1 - \beta = 0.99$. Therefore, the sample consisted of a minimum sample of 390 participants per experiment.

4.7.1.3 Survey Participant Recruitment

AMT was used for participant recruitment and survey distribution. By utilising AMT, this study was able to gain a diverse and rich data set. The invitation to participate in the survey was posted to AMT along with an abstract. Potential respondents could then decide on whether they would participate in the survey, based on the abstract. Respondents could only take the surveys once and were remunerated for their participation if their survey was successfully completed.

4.7.1.4 Sample Demographic

AMT allows researchers access to a larger and more demographically diverse participant pool as compared with the U.S. population (Aguinis et al., 2020). In 2019, there were 250,810 AMT workers worldwide who had completed at least one task in AMT, with more than 226,500 of these workers based in the US (Litman and Robinson, 2017; Moss and Litman, 2019). Buhrmester, Kwang, and Gosling (2011) compared AMT demographics to a large general Internet sample to determine how they compare demographically, and found that AMT respondents were more diverse demographically than the standard Internet sample. The following section describes the demographics of the sample in both experiments.

Experiment 1: Demographic variables of age, nationality, gender and occupation, are outlined in Table 4.11, and are presented across each condition. In the final sample (*n=396*), the gender distribution was 62.1% male (*n* = 246), and 27.9% female (*n* = 150). 60% of the sample fell between the age of 26-40 and over 30% of respondents reported working in management or professional occupations. The completed surveys were equally and randomly distributed across four vignettes, falling in the range of 24.2% to 25.5%.

Table 4.11 Experiment 1 Demographics

		Total Number *(n=396)*	**%**	**Vign 1 *n=101* (25.5%)**	**Vign 2 *n=96* (24.2%)**	**Vign 3 *n=98* (24.7%)**	**Vign 4 *n=101* (25.5%)**
Age	18-25	33	8.5	5	6	13	9
	26-30	84	21.2	19	18	23	24
	31-35	89	22.5	24	20	16	29
	36-40	61	15.4	19	13	15	14
	41-45	33	8.3	10	11	7	5
	46-50	29	7.3	6	9	5	9
	51-55	17	4.3	3	6	5	3
	56-60	28	7.1	7	8	8	5
	61-Plus	22	5.0	8	5	6	3
Nationality	American	389	98.2	100	93	97	99
	Other	7	1.8	1	3	1	2
Gender	Male	246	62.1	61	64	60	61
	Female	150	37.9	40	32	38	40
Occupation	Construction, farming, fishing	19	4.08	4	5	6	4
	Government	28	7.1	8	9	4	7
	Management, professional	139	35.1	35	34	35	35
	Production, transportation	19	4.8	10	6	2	1
	Retired	11	2.8	4	3	4	0
	Sales and office	82	20.7	22	20	15	25
	Service	41	10.4	6	8	12	15
	Student/Unemployed	31	7.8	8	7	8	8
	Other	26	6.6	4	4	12	6

Note: Vign=Vignette

Experiment 2: Demographic variables are outlined in Table 4.12, and are presented across each condition. In the final sample (*n=508*), gender distribution was 60.5% male (*n*=306), and 39% female (*n*=199) with 3 respondents selecting 'prefer not to say'. 60% of the sample fell between the age of 26-40 and over 30% of respondents reported working in management or professional occupations. The completed surveys were equally and randomly distributed across the four vignettes, falling in the range of 24% to 26%.

Table 4.12 Experiment 2 Demographics

		Number ***(n=508)***	**%**	**Vign 1** ***n=130*** **(25.5%)**	**Vign 2** ***n=132*** **(26%)**	**Vign 3** ***n=122*** **(24%)**	**Vign 4** ***n=124*** **(24.4%)**
Age	18-25	31	6.09	7	7	8	9
	26-30	117	23	35	38	22	22
	31-35	112	22	30	17	29	26
	36-40	79	15.5	18	22	19	20
	41-45	46	9	14	11	12	9
	46-50	44	8.6	13	10	11	10
	51-55	36	6.2	5	12	7	12
	56-60	24	4.7	4	4	6	10
	61-Plus	29	5.6	4	11	8	6
Nationality	American	505	99.4	130	131	122	132
	Other	3	.6	0	1	0	2
Gender	Male	306	60.3	86	70	71	79
	Female	199	39.1	43	61	51	44
	Prefer not to say	3	.6	1	1	0	1
Occupation	Construction, farming, fishing.	22	4.8	8	6	5	3
	Government	16	7.1	3	4	3	6
	Management, professional, and related	204	35.1	56	53	51	44
	Production, transportation, and material moving	20	4.8	3	4	8	5
	Retired	16	2.8	4	6	4	5
	Sales and office	100	20.7	22	24	28	26
	Service	53	10.4	13	15	12	13
	Student/Unemployed	34	7.8	12	7	4	11
	Other	40	6.6	9	13	7	11

4.7.2 Experimental Vignette Methodology Design

Experimental research starts with the formulation of a testable hypothesis grounded in a relevant theory, where the researcher then manipulates one or several variables to find out whether they have effect on other variable(s) (Seltman, 2018). An EVM study consists of two key components: first, a vignette experiment as the core component, and second, a traditional survey. The goal of the vignette component is to evaluate what difference it makes when the actual object of study/judgment, or the context in which that object appears, is systematically changed in some way (Mutz, 2011). The goal of the survey component is the parallel/supplementary measurement of additional respondent-specific characteristics, which are used as covariates in the analysis of vignette data (Steiner et al., 2016). The remainder of this section is shaped by the best practice guidelines for EVM studies (Aguinis and Bradley, 2014). The first of these guidelines is to outline the rationale for use of EVM, then the type of EVM, the number and type of vignettes, and the validity criteria are presented.

4.7.2.1 Experimental Vignette Methodology - Rationale

In quantitative research, the combination of the vignette technique with a traditional survey is an effective research method for investigating respondents' beliefs, attitudes, or judgments (Atzmüller and Steiner, 2010). Traditional surveys typically show a high external validity, mainly due to their claim of representativeness and their multivariate measurements (Atzmüller and Steiner, 2010). They also show a low internal validity, caused by the multicollinearity of measured variables and the passive way of taking account of control or explanatory measurements (Atzmüller and Steiner, 2010). In contrast, classical experimental designs derive their high internal validity from orthogonal design plans and an active mode of measurement enabled by a controlled intervention (Atzmüller and Steiner, 2010). Vignette studies try to overcome this by combining the traditional survey with a vignette experiment (Atzmüller and Steiner, 2010). Thus, vignette surveys

have several advantages over traditional surveys. First, since vignettes are representations of subjects or situations, the corresponding questions are embedded in a concrete, realistic context and are thus more realistic (Aguinis and Bradley, 2014). Second, the use of vignettes allows for a simultaneous investigation of the factors varied in the vignette experiment (Steiner et al., 2016). Third, using an experimental design for the vignette experiment provides a high internal validity whilst embedding the vignette experiment in a survey (with random sampling) extends a vignette experiment's external validity at least to the survey's target population (Steiner et al., 2016).

EVM allows researchers to include factors that are relevant to the research question while excluding those that might confound the results (Aguinis and Bradley, 2014). By helping to test causal hypotheses that would otherwise be difficult, EVM is particularly useful in domains where variables are known to correlate (Aguinis and Bradley, 2014). Privacy concern is already found to be negatively associated with trust (Arpaci, 2016; Bansal and Zahedi, 2015; Hong and Thong, 2013; Malhotra et al., 2004; Bandara et al., 2020), behavioural intentions (Fortes and Rita, 2016; Thakur and Srivastava, 2014), and privacy awareness (Warner and Wang, 2019). Thus, EVM is considered suited to exploring privacy in the context of the nonmarket environment.

4.7.2.2 Experimental Vignette Methodology - Type

The next major decision in EVM design is to choose the type of EVM. The major options involve paper people and policy capturing/conjoint analysis. Paper people studies consist of presenting participants with vignettes typically in written form, and asking participants to make explicit decisions, judgments, choices or preferences (Aguinis and Bradley, 2014). Policy capturing and conjoint analysis studies present respondents with scenarios containing carefully manipulated variables; however, in contrast to paper people studies, participants are asked to make decisions between scenarios in order to capture implicit

processes (Aiman-Smith et al., 2002). Paper people studies have been used widely in a variety of research domains such as entrepreneurship (e.g., Bucar et al., 2003), organizational citizenship behaviour (e.g., Podsakoff et al., 2011), and ethics (e.g., Hoyt et al., 2013). This type of EVM is most appropriate when the goal is to assess explicit processes and outcomes—those about which participants are aware and on which they can provide information (Aguinis and Bradley, 2014). The type of EVM used in this study is a paper people type – as both experiments focus on participant's explicit responses to hypothetical scenarios.

According to Atzmüller and Steiner (2010), once the type of EVM is decided, the research design should then be decided. Choices include a between-person, within-person, or mixed research design (Atzmüller and Steiner, 2010). The between-person design requires that each participant read only one vignette, and comparisons are made across participants (Atzmüller and Steiner, 2010). For a within-person design, each participant views the same set of vignettes, and comparisons are made between vignettes within the same person (Atzmüller and Steiner, 2010). In mixed designs, different groups of participants receive different sets of vignettes; however, within each group, participants see the same vignettes (Atzmüller and Steiner, 2010). The chosen research design here is a between-person design. For between-person designs, Aguinis and Bradley (2014) highlight that without other vignettes to serve as referent points, responses may not accurately reflect the true judgments of each respondent. Therefore, in between-person designs, it is important that all participants be provided with as much contextual baseline information as possible (Aguinis and Bradley, 2014).

4.7.2.3 Number of Vignettes and Vignette Design

The next decision in the EVM is to decide on the number of vignettes in the vignette 'pool', as dictated by the study's purpose (Weber, 1992). Best practice guidelines for

studies applying an EVM method suggest limiting the number of vignettes a participant must read, for two reasons. First, multiple vignettes can invoke vignette response fatigue (Hughes and Huby, 2002). Second, multiple vignettes can present issues with order or interaction effects (O'Connor and Hirsch, 1999) and thereby confound study results (Zellman, 1990). To minimise the confounding factors that can contaminate experimental results, each participant in this study will be exposed to only a single vignette, randomly selected from a pool of four vignettes, where each vignette represents one experimental treatment.

Experiments have to fulfil two fundamental conditions. First, "no causation without manipulation" (Imai, 2017. p. 48), i.e., researchers must have control over the manipulation of variables. They must be able to "isolate causal variables that constitute the basis for experimental manipulation" (Iyengar, 2011, p. 78). Second, researchers need to rule out the fundamental problem of causal inference, i.e., our inability to observe the counterfactual outcomes (Imai, 2017). The way to accomplish this is to use random assignment of participants to conditions, ensuring that each participant has an equal chance to be in each treatment condition. Thus, in this study each participant is first presented with baseline background describing both the organisation and their relationship with the organisation. The participant is then randomly assigned one of four possible vignettes, called a treatment condition. These vignette baselines and treatment conditions are discussed below.

Vignette Baselines: The first part of the vignette outlines the context of the scenario and is unchanged throughout the experiment. Each vignette baseline describes the nonmarket privacy activity of a fictitious large technology organisation called ModernTech. This organisation replicates (i) the type of organisation with a financially powerful lobby, and (ii) an organisation with dependence on, and historical use of, consumer data. It has been

shown that the levels of privacy needs and concerns are dependent on the type of information collected and used by an organisation (Milne and Gordon, 1993; Phelps et al., 2000; Sheehan and Hoy, 2000; Malhotra et al., 2004). Malhotra et al. (2004) refer to this information attribute as 'information sensitivity'. In the first experiment, the baseline describes a scenario where the reader is informed that they have provided personal financial information to an organisation. In the second experiment, the baseline is contextualised around an email system, which the reader is informed potentially has information related to their friends, financial institutions, public agencies and health institutions etc. In both experiments, the consumer should understand that they have had experience with the organisation, and the nature of the information collection by the organisation. Hence 'experience with the organisation' together with 'sensitivity of the information' is expressly stated in the baseline of both experiments.

In the first experiment, the baseline text is:

"ModernTech is a (fictitious) large North American technology organization, providing online services/products to 50 million customers. ModernTech has to process certain consumer data in order to complete a transaction (e.g. credit card details, expiry dates and transaction details) or in order to register an account (such as name, date of birth, address, email etc). Imagine that you recently purchased a repeating monthly subscription to use one of ModernTech's mobile applications and you have disclosed information to ModernTech during this purchase, such as your credit card details, your email address and your mobile phone number".

In the second experiment, the baseline text is:

"ModernTech is a (fictitious) large North American technology organization, providing subscription-based email systems to 40 million customers across the United States. Imagine that in 2020, a new law was introduced called the Federal Data Surveillance Act. This law, which was introduced to enhance national security and anti-fraud measures, allows government agencies to access personal data on-demand, in organisations such as ModernTech. Imagine that you recently set up and registered to use an email account with ModernTech, and you often use this account to send personal emails such as those to your friends, family, financial institutions, public agencies and health institutions etc."

Vignette Treatment: The next part of the vignette is the treatment condition. Experimental treatments are "potentially causal interventions" that are controlled by a researcher (Druckman et al., 2011, p. 16). The treatment condition aims to manipulate the independent/predictor variable which is the "the principal variable that we expect to have a causal impact" (Morton and Williams, 2010, p. 76). Its value is independent from other variables in the experiment and instead is manipulated by the researcher.

The vignettes which follow the baseline describe a NMPv activity. In the Online Delphi Survey, the panelists classified and weighted certain NMPv activities, in terms of the levels of control and justice signalled by them (see section 4.5.3). For instance, NMPv lobbying that benefits the organisation more than the consumer was classified as a control activity, and NMPv lobbying that benefits the consumer more than the organisation was classified as a justice activity. Therefore, in both experiments the variable being manipulated is the beneficiary of the NMPv activity – mirroring a justice-based or control-based NMPv activity. In each experiment, the vignette baseline is followed by a randomly selected vignette from a pool of four vignettes. The four vignettes are almost identical, however the beneficiaries of the NMPv activity are manipulated in each vignette (this manipulated variable is referred to during analysis, as 'ManBnf'). In the first experiment the context of the experiment is a CPA, whereas, in the second experiment, the context is adjusted to include an activity that is either a CPA or a CSR.

Table 4.13 illustrates the manipulation involved in the first experiment and Table 4.14 illustrates the manipulation involved in the second experiment.

Table 4.13 Experimental Vignette Treatment Condition: Experiment 1

Theory			Manipulation						Vignette Text
			Beneficiary			Non-Beneficiary			
Vignette Context	Control	Justice	Organisation	Consumer	Individual	Organisation	Consumer	Individual	
1 (CPA)	High	-	X				X		*ModernTech is not supportive of proposals for a new privacy regulation, called The Ultimate Privacy Act, which requires that organisations provide a 'Do Not Sell or Share My Data' option to their consumers. ModernTech objects to these requirements, as they would reduce the amount of data ModernTech can share/sell and would therefore negatively impact their efforts to maximize profit.*
2 (CPA)	High	-	X					X	*ModernTech is not supportive of proposals for a new privacy regulation, called The Ultimate Privacy Act, which requires that organisations provide a 'Do Not Sell Or Share My Data' option to their consumers. Lawmakers have suggested that these requirements be extended in due course to all individuals in society e.g., taxpayers, website visitors, patients, students etc. ModernTech objects to these requirements, and objects to extending these requirements to all individuals in society, as these proposals would reduce the amount of data that ModernTech can share/sell, and therefore negatively impact their efforts to maximize profit.*
3 (CPA)	-	High		X		X			*ModernTech is supportive of proposals for a new privacy regulation, called The Ultimate Privacy Act, which requires organisations to provide a 'Do Not Sell Or Share My Data' option to their consumers. Although ModernTech accepts that these requirements will reduce the amount of data they can share/sell (and therefore negatively impacts their efforts to maximize profit), ModernTech recognizes the importance of strengthening privacy regulation for consumers.*
4 (CPA)	-	Higher			X	X			*ModernTech is supportive of proposals for a new privacy regulation, called The Ultimate Privacy Act, which requires organisations to provide a 'Do Not Sell Or Share My Data' option to their consumers. Lawmakers have suggested that these requirements be extended in due course to all individuals in society e.g., taxpayers, website visitors, patients, students etc. Although ModernTech accepts that these requirements will reduce the amount of data they can share/sell (and therefore negatively impacts their efforts to maximize profit), ModernTech also recognises the importance of strengthening privacy regulation for society, and therefore supports extending these requirements to all individuals.*

Table 4.14 Experimental Vignette Treatment Condition: Experiment 2

Theory			Manipulation				Vignette Text
			Beneficiary		Non-Beneficiary		
Vignette Context	Control	Justice	Organisation	Consumer	Organisation	Consumer	
1 (CSR)	High	-	X			X	*After hypothetically setting up and using ModernTech's email system, we would like you to imagine that you read the following information regarding ModernTech:* *"ModernTech responds to all requests for consumers personal information made by the government under the Federal Data Surveillance Act, as it helps ModernTechs compliance obligations".*
2 (CSR)	-	High		X	X		*After (hypothetically) setting up and using your ModernTech email account, we would like you to imagine that you read the following information regarding ModernTech:* *"ModernTech refuses to comply with government requests for personal information made under the Federal Data Surveillance Act, as it interferes with the consumer's right to privacy".*
3 (CPA)	High	-	X			X	*After (hypothetically) setting up and using your ModernTech email account, we would like you to imagine that you read the following information regarding ModernTech:* *"ModernTech lobbies government in support of the requirements of the Federal Data Surveillance Act, as it helps with ModernTech's compliance obligations".*
4 (CPA)	-	High		X	X		*After (hypothetically) setting up and using your ModernTech email account, we would like you to imagine that you read the following information regarding ModernTech:* *"ModernTech lobbies government against the Federal Data Surveillance Act, as it interferes with the consumer's right to privacy"*

4.7.3 Experimental Vignette Methodology Survey

After the experimental baseline and vignettes are presented, a survey is then presented to participants. The following sections detail the survey structure, the survey measures, the quality criteria, and the ethical considerations.

4.7.3.1 Survey Structure

The survey was conducted consistent with the ethical principles of the Declaration of Helsinki (World Medical Association, 2013). Informed consent was obtained from participants. Data collection occurred during April 2020 for Experiment 1, and February 2021 for Experiment 2. Copies of the surveys for both experiments can be found in Appendix L and Appendix N. Both surveys were comprised of the following sections in the order recommended by Aguinis and Bradley (2014):

Section I:	Plain Language Statement, Informed Consent, Demographics
Section II:	Base Vignette and a Treatment Vignette
Section III:	Variables: Privacy Concern
	Variables: Consumer Trust
	Variables: Purchase/Continuance Intention
	Variables: Privacy Awareness (Experiment 2 only)
Section IV:	Control Variables

In both experiments, the respondent is presented first with the plain language statement, informed consent and demographic measures, i.e., age, gender, occupation, nationality, similar to Martin (2016). The collection of sociodemographic measures is important for the analysis of vignette data because they help in investigating heterogeneous response behaviours and in reducing the error variance at the respondent level (Steiner et al., 2016). These measures have also been found to influence privacy concern and trust (Benamati et al., 2017). Although participation was limited to US AMT workers only, nationality was included

in order to identify someone who identified with a different nationality but was resident in the US. The dependent variables follow, i.e., privacy concern, consumer trust, and purchase intention/continuance intention. To avoid any priming bias, each of the measurement items were also randomly presented to the participant. Finally questions regarding control variables are then presented. Attention checks, manipulation checks, and bot detection checks are included throughout both surveys. Embedded survey logic is configured to detect failed responses to these checks, and to end the survey where these checks are failed.

As the endogenous variables were measured at the same time, this can generate fears regarding common method bias (CMB). However, various procedural remedies recommended by MacKenzie et al. (2011) were applied during survey design. These remedies include separating endogenous and exogenous variables, offering descriptions of terms and technologies, ensuring all items were unambiguous, notifying respondents that there were no right or wrong answers, and guaranteeing anonymity. In addition to this, in each section, scale items were presented in a random order. When scales are presented one by one, this may push people to provide the same answers to all the items of the first scale, then the same answers to all items of the second scale and so on (Diefendorff et al., 2016; Podsakoff et al., 2003).

4.7.3.2 Measurement of Variables

This section discusses the measurement of variables in the survey. The items were adapted from previously validated scales. Due to the application of variables in the context of the vignette scenario, many items required slight rewording, including using ModernTech as the name of the organisation, where relevant. With the exception of political affiliation measures, participants were asked to indicate their level of agreement on a five-point Likert scale ranging from ‘strongly disagree’ to ‘strongly agree’. First discussed are the dependent variables, followed by the moderator variables and then the control variables.

Dependent Variables

Privacy concern: The four-item Likert scale from Dinev and Hart (2004) was used in Experiment 1. The term *'my credit card details will be stolen'* was changed to '*the information I provide to ModernTech such as my financial details, will be stolen'* as this better reflected the multiple mechanisms used for payments such as PayPal, Revolut and Electronic Transfers. Experiment 2 draws on the Mobile User Information Privacy Concern (MUIPC) scale from Xu et al. *(*2012) to operationalise nonmarket privacy concern as a three-dimensional construct (misuse, surveillance and intrusion) relating to concerns about the loss of privacy in an online email application (rather than a mobile application). This scale reflects two important dimensions of privacy concern important to the experimental vignettes – perceived intrusion and perceived surveillance. These items were derived from Xu et al. (2012) in the context of mobile applications and therefore the items were adapted from mobile application to suit an email application. For example, an item measuring the perceived intrusion dimension "*I feel that as a result of my using mobile apps, information about me is out there that, if used, will invade my privacy"* was changed to "*I feel that as a result of my using online email systems, information about me is out there that, if used, will invade my privacy*".

Consumer trust: The four-item Likert scale from Fogel and Nehmad (2009) measured the extent to which a consumer felt they trusted ModernTech. The words 'Facebook' were replaced with 'ModernTech'. For example, to measure the trustworthiness dimension of ability: '*I could count on ModernTech to protect customers' personal information from misuse'.*

Purchase intention/continuance intention**:** In this study, intentions are conceptualised as the likelihood that a consumer will engage in a desired behaviour, including making future

purchases, or continuing to engage with an organisation. This four-item Likert scale measured the extent to which a consumer had positive inclinations with regard to purchasing products from ModernTech. In Experiment 1, purchase intention was measured using the purchase intentions scale (Pavlou, 2003) derived from Chieh-Peng et al. (2011). Again, the items were modified to specifically mention ModernTech – for example: *'Given the chance, I predict that I may purchase from ModernTech in the future'.* In Experiment 2, the vignettes shaped a hypothetical scenario where the respondent was already using ModernTech's email system, and the researcher wanted to measure the respondents inclination to continue to use ModernTech's email system. Therefore, in Experiment 2, the consumer's future use attitude toward ModernTech was measured using a three-item Likert scale called Intentions to Continue Use of an IS System, derived from Bhattacherjee (2001). Again, the items were modified to specifically mention ModernTech "*My intention would be to continue using ModernTech's email system",* and to specifically mention the actions they would continue to do i.e., " *to send emails to my friends, family, doctor and other personal connections".*

Moderator Variables

Privacy Awareness: In Experiment 2, privacy awareness was measured using a four item Likert scale derived from Xu et al.'s (2008) study on the formation of individual privacy concern, and adapted by Warner and Wang (2019). Privacy awareness beyond an organisation's privacy practices is determined with questions such as *"I am aware that my personal information could be made available to government agencies".* Again the items were modified to specifically mention ModernTech and to specifically mention data privacy in the US, as the sample were US respondents*:" I am aware of the wider issues around data privacy within the US from the news and other sources".*

Control Variables

Dispositional factors commonly considered important for privacy concern and for trust were controlled for, namely disposition to value privacy and propensity to trust. Disposition to value privacy is included as a control variable to disentangle that an individual's level of privacy concern did not depend on an underlying general attitude towards privacy. Included in the control section of both experiments is a three-item Likert scale adapted from Xu et al. (2011). This scale contained items such as "*Compared to others, I am more sensitive about the way companies handle my personal information".*

Propensity to trust is included as a control variable to disentangle that levels of consumer trust in the experiment did not depend on an underlying general willingness to trust others. Propensity to trust was measured separately using a four item Likert scale which contains two items from Lee and Turban (2001) and two items from McKnight et al. (2002). These scales were combined and applied by Frazier et al. (2013) and included items such as *'My typical approach is to trust new acquaintances until they prove I should not trust them'.*

The presence of government surveillance can be considered a beneficial factor or non-beneficial factor depending on the individuals perceived need for government surveillance (Dinev et al., 2008) and their political orientation (PEW Research Centre, 2015; Regan et al., 2013). Therefore, perceived need for government surveillance and political orientation were also controlled for in Experiment 2. The perceived need for government surveillance is a four-item Likert scale from Dinev et al. (2008) and is unchanged. It contains items such as *"The government needs to have more authority to use high tech surveillance tools for peoples online activities".*

A set of two political affiliation questions are derived from Talhelm et al. (2015) and also remain unchanged. The first is a social question "*How would you describe your political outlook with regard to social issues such as marijuana legalization, abortion, personal*

freedoms and gay rights?", and the second is an economic question "*How would you describe your political outlook with regard to economic issues such as how governments should regulate trade and taxes, how much the government should tax income and whether the government should regulate businesses?"*. The scale for those questions ranges from 1 = very liberal to 7 = very conservative, with 4 = moderate. This lets libertarians separate themselves out from social conservatives, as libertarians often identify as social liberals but economic conservatives (Talhelm et al., 2015).

4.7.4 Statistical Data Analysis Strategy

For between-person designs, the Analysis of Variance (ANOVA) test is recommended (Atzmüller and Steiner, 2010). ANOVA is an inferential statistical test that allows one to test if each of several independent variables have an effect on the dependent variable. ANOVAs are useful for testing for significant differences between categorical predictors (such as those included in a vignette design) on continuous outcome variables. In an experiment, an ANOVA is considered more effective than, for instance, a t-test, as every t-test has a chance of a Type I error (error is usually 5%). By running two t-tests on the same data this increases the chance to 10% and so on. An ANOVA controls for these errors so that the Type I error remains at 5% thus providing more confidence. An ANOVA test can be one-way or two-way, which refers to the number of independent variables (IV) in the ANOVA test. A variation of ANOVA, called Analysis of Covariance (ANCOVA), is a general linear model blending ANOVA and regression. It takes the unexplained within-group variances from the ANOVA test and tries to explain them with confounding variables, or other covariates (Overall, 1993; Senn, 1994; Senn, 2006). ANCOVA evaluates whether the means of a dependent variable (DV) are equal across levels of a categorical independent variable (IV) often called a treatment, while statistically controlling for the effects of other continuous variables that are

not of primary interest, known as covariates (Keppel, 1991). Mathematically, ANCOVA decomposes the variance in the dependent variable into variance explained by the covariate, variance explained by the categorical independent variable, and residual variance. Intuitively, ANCOVA can be thought of as 'adjusting' the dependent variable by the group means of the covariate(s) (Keppel, 1991). Whilst multiple possible covariates can be used, the more covariates entered, the fewer degrees of freedom presented. Entering a weak covariate will reduce the statistical power. Strong covariates have the opposite effect and can increase the power of the test. Statistical power is important in order to draw accurate conclusions about a population using sample data (Greenland et al., 2016).

ANCOVA can also be used in pre-test/post-test analysis when regression to the mean affects post-test measurement (Bonate, 2000). ANCOVA can also be used to study combinations of categorical and continuous variables, or variables on a scale as predictors (Leech et al., 2005). The research design path thus leads towards a one-way ANOVA. The Tukey test for comparison of means across vignettes is used, ANCOVA is used to test for covariates, and a two-way ANOVA, achieved via linear regression, is used to test for moderation. SPSS (v27) is used to run the statistical tests. Microsoft EXCEL is used to clean the data of incomplete records, and to produce charts from SPSS output. The PROCESS macro from Andrew Hayes (2018) is used to produce the moderation data matrix – in order to plot the moderation effects for Experiment 2.

4.7.5 Quality Criteria

Surveys contain potential weaknesses including length restrictions, possibility of missing data, non-response to some items, possibility of social desirability, and low response rates (Johnson and Turner, 2003). Bearing that in mind, this survey was designed in ways which limit these weaknesses. Only important variables were included to limit the length, and only

complete responses were used in analysis. Instructions and descriptions were worded neutrally to limit any possible social desirability effects. As many of the variables were tested in the context of NMPv for the first time, extensive pilot testing was conducted. The quantitative data underwent extensive testing to ensure internal and external validity, and reliability thresholds were met, in line with recommendations (Venkatesh et al., 2013; Straub et al., 2004). First, to establish validity and comprehension, the survey scales of both surveys underwent face validity tests conducted by a panel of experts. Second, to enhance validity, the surveys were pilot tested on a number of small groups (Johnson and Turner, 2003). Initially, the survey was piloted among a group of academics with expertise in survey development. These experts provided advice on the minor rewording of items, and clarifying section descriptions. The survey was refined based on this feedback.

4.8 Integration

In mixed methods research, there are a number of specific approaches to integrate qualitative and quantitative research procedures and data (Creswell et al., 2010). These approaches can be implemented at the design, methods, and interpretation and reporting levels of research. Table 4.15 presents an overview of mixed methods integration approaches, adapted from Fetters et al. (2013).

Table 4.15 Levels of Integration in Mixed Methods Research (adapted from Fetters et al., 2013)

Approach	Types and Summary	
	1. Integration Level : Design	
Basic Designs	Exploratory Sequential	The researcher first collects and analyses qualitative data, and these findings inform subsequent quantitative data collection.
	Explanatory Sequential	The researcher first collects and analyses quantitative data, then the findings inform qualitative data collection and analysis.
	Convergent (Concurrent)	The qualitative and quantitative data are collected and analyzed during a similar timeframe. An interactive approach may be used where iteratively data collection and analysis drives changes in the data collection procedures.
Advanced Frameworks	Multistage	Researchers use multiple stages of data collection that may include various combinations of exploratory sequential, explanatory sequential, and convergent approaches
	Intervention	Qualitative data are collected to support the development of an intervention, to understand contextual factors during the intervention that could affect the outcome, and/or explain results.
	Case study	Both qualitative and quantitative data are collected to build a comprehensive understanding of a case, the focus of the study.
	Participatory Community-based	Involves the voices of the targeted population in the research to inform the direction of the research.
	2. Integration Level : Methods	
Connecting	One database links to the other through the sampling frame.	
Building	Results from one data collection procedure informs the data collection approach of the other procedure, the latter building on the former e.g., Items for inclusion in a survey are built upon previously collected qualitative data.	
Merging	The two databases are brought together for analysis and comparison.	
Embedding	Embedding may involve any combination of connecting, building, or merging, but the hallmark is recurrently linking qualitative data collection to quantitative data collection at multiple points.	
	3. Integration Level : Interpretation and Reporting	
Narrative Weaving	Researchers describe the qualitative and quantitative findings in a single or series of reports through Weaving, Contiguous or Staged approaches.	
Data Transformation	First, one type of data must be converted into the other type of data (i.e., qualitative into quantitative or quantitative into qualitative). Second, the transformed data are then integrated with the data that have not been transformed.	
Joint Display	Researchers integrate the data by bringing the data together through a visual means to draw out new insights beyond the information gained from the separate quantitative and qualitative results.	

Reflecting the levels of integration from Fetters et al. (2013), integration is presented in the following ways:

- At the design level, results from the Online Delphi Survey are fully integrated into the qualitative analysis of Study One.
- At the methods level, results from the Online Delphi Survey inform the survey used in the EVM of Study Two, and therefore adopts the 'building' approach to methods integration,
- At the interpretation and reporting level, data from both Study One and Study Two are jointly discussed through the reporting narrative.

4.9 Chapter Conclusion

In this chapter, the philosophical and methodological underpinnings of this research and related considerations were outlined. The justification for pragmatism as a philosophical approach was presented together with a justification for a mixed methods research design. The overall research strategy was then discussed. First, an Online Delphi Survey was conducted, involving a panel of experts and a survey, to refine and validate the qualitative research framework. Second, using the Fortune 100 index, sixty five CSR reports were then collected, and thematic analysis applied to these reports to determine an organisation's privacy orientation. Finally, an EVM based survey, using AMT, was conducted to explore and compare the influence that privacy in the nonmarket has on consumers. As mixed methods studies are often critiqued for being less rigorous than single method studies (Morse, 2003), both the quantitative and qualitative components included an outline of the rigorous testing and analysis undertaken, prior to the integration of the data. The chapter concluded with an outline of the integration of the three stages of the research at design, methods, and reporting levels. The next chapter discusses the qualitative study, and discusses the application of thematic analysis, together with the findings, along with the methods used to validate the data.

5 CHAPTER FIVE: STUDY ONE – QUALITATIVE ANALYSIS

5.1 Introduction

Study One responds to RQ1 and RQ2. The first aim of Study One is to develop a coding framework, characterised by levels of control and justice signalled by NMPv activities, that can be used to position an organisation's NMPv orientation. This is achieved using an Online Delphi Survey, as outlined in Section 4.6.3.1. The second aim is to demonstrate operability of the coding framework, by using it to analyse the reported NMPv activities of a sample of organisations. This is achieved using the thematic analysis of a sample of CSR reports. This chapter focuses on presenting the results of Study One's qualitative analysis of a sample of CSR reports. The chapter begins with an overview of the qualitative analysis procedures, outlining the steps involved in the thematic analysis. The themes reported in the CSR reports are then discussed. The chapter concludes with a discussion of the NMPv orientations of the organisations in the sample.

5.2 Qualitative Analysis Procedures Overview

The thematic analysis in Study One uses a four-step framework, guided by Braun and Clarke's (2006) framework for thematic analysis. A deductive approach to thematic analysis is conducted using a codebook previously developed during the Online Delphi Survey. Figure 5.1 illustrates the steps taken.

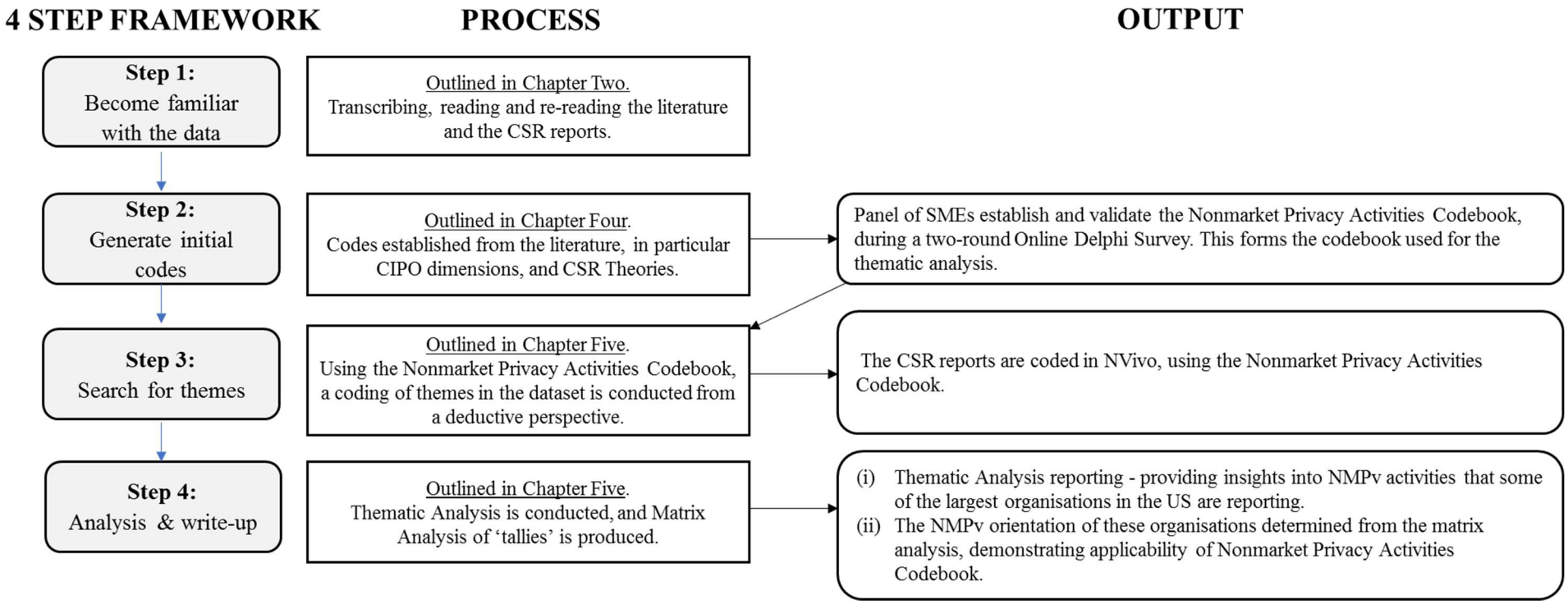


Figure 5.1 How Braun and Clarke's (2006) Framework for Thematic Analysis was Conducted

5.2.1 Step 1: Familiarisation

The researcher reviewed the nonmarket environment literature, together with the privacy literature to gain insight into the types of approaches to privacy, and to understand the activities associated with those approaches, covered in detail in Section 2.5. The researcher then reviewed the CSR reports in the sample to understand their structure and general content. During this report review stage, the researcher noted the words typically used to describe privacy in the CSR Reports, such as data protection, data privacy, privacy, data security. Furthermore, the researcher became familiar with the structure of the CSR reports – as many were constructed in line with the Global Reporting Initiative (GRI) and International Standards Organisation (ISO) guidelines for CSR reporting. For example, when an organisation followed a reporting standard such as GRI or ISO, this was typically noted at the start of the report. These types of reports contained a section on the number of reported customer privacy breaches, and their first reference to privacy was often in a section called 'materiality assessments'. A materiality assessment is the process of identifying, refining, and assessing numerous potential environmental, social and governance issues that matter most to an organisation and its key stakeholders, and condensing them into a short-list of topics (and typically a chart) that inform organisational strategy, targets, and reporting (KPMG, 2013).

5.2.2 Step 2: Code Generation

A theme may be initially generated inductively from the raw data or generated deductively from theory and prior research (Boyatzis, 1998). The generation of an initial set of codes for the Nonmarket Privacy Activities Codebook was first derived deductively from prior research i.e., from the activities outlined by Pollach (2011) and Allen and Peloza (2015), from the legal, strategic and ethical dimensions of the CIPO (Greenaway et al*.,* 2015), and from the researcher's outline of an evolution of perspectives of NMPv and associated

NMPv activities over the last four decades. To enhance the quality of the theme/code development process, an Online Delphi Survey (Linstone and Turoff, 2002) was introduced and is detailed in Section 4.5.3.1.

5.2.3 Step 3: Search for Themes

In this study, the thematic analysis takes a deductive approach using a codebook. Deductive analysis is driven by the researcher's theoretical or analytic interest, typically involving a codebook, and may provide a more detailed analysis of some aspect of the data but tends to produce a less rich description of the overall data (Braun and Clarke, 2020). The codebook approach to thematic analysis is useful for researchers conducting a realist, deductive, thematic analysis (Fereday and Cochrane, 2006), aligning epistemologically and ontologically with the researcher's philosophical paradigm, to apply the most pragmatic approach to explore the research questions. The researcher accepts that whilst a deductive approach may provide a more detailed analysis of certain aspects of the data (in this case, themes of control and justice) it can produce a less rich description of the overall data (Braun and Clarke, 2006). However Study One does not seek to find the richest description of the overall data, and instead seeks to determine if the organisation's NMPv orientation can be determined using levels of control and justice signalled by an organisation's NMPv activities. Therefore, a systematic deductive coding approach was conducted, using the Nonmarket Privacy Activities Codebook as the codebook. In this way, control and justice are the key themes, and the NMPv activities associated with control and justice, are the subthemes.

CSR reports typically provide details on topics related to environment, climate, governance and social issues. Typically they begin with a letter from a corporate executive, such as the president, chief executive officer, or chief sustainability officer, then a table of contents (Cote, 2021). Reports can vary in length, and typically range between 40 and 200 pages

long (Cote, 2021). The reports were searched for keywords that would lead to sections related to privacy. As previously noted, privacy and data protection are interpreted differently in the US and in Europe, therefore the reports were first searched using the keywords: ‘privacy’ and then ‘data protection’. The reports were also searched using the terms ‘cybersecurity’ and ‘governance’, as these terms often contained references to encryption and other privacy enhancing tools. Sixty five reports were found to reference privacy in this way. References to privacy varied in size, from one line to multiple pages. Where a CSR report was formatted in line with a structured CSR Reporting standard such as GRI, a minimum of a paragraph would be dedicated to discussing privacy.

Once a keyword was found – the section was compared with the codebook to determine if the text reflected a code. When a text reflected a code, the text was coded using NVivo. More than one code could be assigned to a text. This process continued until all the reports were coded. By way of explanation of the coding process, examples of coding are outlined in Table 5.1.

Table 5.1 Examples of the Coding Process

Organisation	Text	Coded at Theme	Coded at Subtheme	Researcher Justification
American Airlines (2019, p. 28)	*"... the privacy program is run by the Global Privacy Office, it is a team effort with involvement from senior leaders on the Privacy Council, Privacy Liaisons who are members of key business units, and all of our team members who are trained and responsible for adhering to American's privacy requirements, which we base on applicable laws".*	Control	DrivnByComplnce	The organisation's privacy requirements are based on applicable laws.
		Justice	MaxStaff4Priv	The organisation reports 'privacy liaisons' in each business unit, a privacy team, a Global Privacy Office, the involvement of senior leadership, and a privacy council.
AT&T (2019, p. 16)	*"with the Center for Democracy and Technology, the Future of Privacy Forum, the Information Accountability Foundation, Access Now, Red en Defensa de los Derechos Digitales, ARTICLE 19 and RightsCon".*	Justice	CollabAdvocacyGrps	The Future of Privacy Forum is a non-profit organisation for privacy leadership and scholarship, regarding principled data protection practices in support of emerging technologies.
FedEx (2019, p. 20)	*"We take precautions to safeguard all personal data and ensure a secure environment, including customer transactions".*	Control	TransFocused	The text specifically highlights customer transactions.
IBM (2019, p. 12)	*"IBM has called for a precision regulation approach to addressing Americans' privacy concerns and has actively encouraged the U.S. Congress and governments worldwide to make privacy protections a priority".*	Justice	LobbyBenefitSociety	The text refers to addressing the privacy concerns of 'Americans', rather than customers, or the organisation.

5.2.4 Step 4: Analysis and Write Up

This study adopts two different approaches to thematic analysis (King and Horrocks, 2010) thus Step 4 is divided into two sections. First, the results of the traditional codebook-based approach to thematic analysis are presented. Then the results of the matrix approach to thematic analysis (Brooks et al., 2015; Groenland, 2018; Miles and Huberman, 2013; Nadin and Cassell, 2004) is presented. A matrix characterises the intersection of two lists, set up as rows and column (Miles et al., 2014). In this study, the matrix consists of rows representing themes and subthemes, and columns representing CSR reports. The matrix is generated using NVivo and populated with the number of occurrences of the themes and subthemes coded for each CSR report.

5.2.4.1 Thematic Analysis: Control Themes

The theme of control and its associated subthemes are presented in Table 5.2, outlining how each subtheme is reported in the CSR dataset and the weighting assigned to the subtheme i.e., the results from round 2 of the Online Delphi Survey. This weighting determines 'how much' control a subtheme signals, and is used in later analysis to weight the tallies of subthemes occurring in the dataset. Certain subthemes were not reported in the CSR reports as they had a score of zero, namely:

- Limited staff assigned to privacy
- Limited budget assigned to privacy
- Stakeholders are not privacy aware
- Low profile non executives assigned to privacy
- Privacy is directed at improving stockholder share value

Whilst these are removed from the results, this does not mean that these subthemes are unimportant to the coding framework, but rather that these themes do not emerge from the CSR reports.

Table 5.2 Examples of Control Subthemes

Subtheme	Weight	Example	No. Rports	No. Refs
The organisation's privacy activities are aimed only at external stakeholders.	1	**Kroger (2020, p. 38)**: *"We encourage our customers to use complex passwords and to change them regularly".*	32	51
The organisation's privacy activities are aimed only at internal stakeholders.	1	**Allstate (2019, p. 26)**: *"…implemented an annual compliance confirmation process that requires every employee to complete annual mandatory training courses and agree to follow appropriate company policies".*	33	51
The organisation's privacy activities are driven by compliance.	1	**Valero (2019, p. 66):** *"We promote an organisational culture focused on regulatory compliance".*	50	158
The organisation is transaction-focused.	3	**Best Buy (2019, p. 37):** *"We are committed to protecting the privacy of our customers' information by using a variety of information security measures to protect their transactions".*	10	11
The organisation does not publish its privacy values.	3.5	N/A	28	28
Lobbying governments for privacy standards that are most beneficial to the organisation.	4	**HP (2019, p. 31):** *"The secure movement of data is essential to our business, …. our privacy and government relations teams work with governments worldwide to develop robust and globally interoperable privacy regulations".*	1	1
Ownership is shared between the individual and organisation - however the organisation expresses greater ownership.	4	**Cigna (2019, p. 18):** *"Our privacy and information protection risk management framework is a shared risk model, which strives to further integrate our privacy, information protection, and related enterprise risk management functions the security and privacy of customer and employee data is absolutely fundamental to our license to operate".*	5	7
The organisation is data-focused.	5	**Ford (2020, p. 53):** *"Harnessing the data provided by connected vehicles and using it to create even better experiences continues to be a key priority".*	6	12
The organisation is inference-focused.	5	**Goldman Sachs (2019, p. 23):** *"…in 2019 we partnered with Apple to launch a no-fee credit card that incorporates new levels of privacy, security and transparency, and provides tools to analyse spending patterns and show customers how to save on interest".*	2	2
The organisation operates as an Information Owner.	5	**General Motors (2019, p. 78):** "We utilize an opt-in approach where legally required based on the nature of the data collected and its intended use".	5	5

The most frequently occurring control subthemes were

- Privacy is driven by compliance
- No privacy values published in their CSR report
- Privacy is aimed at external stakeholders/internal stakeholders

These subthemes are discussed in the remainder of this section.

Privacy is Driven by Compliance

A weighting of '1' was assigned to NMPv activities that were driven by compliance. This indicates that these activities signal low levels of control. 77% of organisations *(n=50)* reported NMPv activities driven by compliance. There were 158 references to compliance-focused NMPv activities, making this the most referenced privacy activity in the Nonmarket Privacy Activities Codebook. For example, Delta reported:

> *"We and other U.S. carriers are subject to laws regarding the protection privacy of customer and employee data that vary between the countries in which we operate. We continue to update our processes to adhere to domestic and international privacy and data protection laws and regulations."* (Delta, 2019, p. 65).

Even organisations in high-justice NMPv orientations (which we discuss later in the Chapter) such as Apple, Verizon, IBM and HP, also reported NMPv activities that were driven by compliance, however these organisations also reported NMPv activities exceeding compliance – indicating that for these organisations compliance is a baseline, rather than the goal. For example, HP reported:

> *"Breaches of customer privacy cover any noncompliance with existing legal regulations and voluntary standards regarding the protection of customer privacy related to data for which HP is the data controller"* (HP, 2019, p. 31).

This is consistent with extant suppositions that the need to control information extends beyond just the consumer's need, to include the control needs of other key stakeholders - such as the organisations themselves, society and governments (Hughes, 2012). Control

cannot be exercised by an individual without the organisation putting an architecture of control in place such as a regulated set of structural measures that aim to secure individual's personal data, namely technological controls and organisational controls (Lazaro and Le Metayer, 2015).

No Privacy Values Published in the CSR report

Where an organisation did not report their privacy values, the SMEs assigned a weighting of '3.5'. This is the only entry in the Nonmarket Privacy Activities Codebook that refers to an 'absence' of an NMPv activity rather than the 'occurrence' of an activity. A weighting of 3.5 indicates that this subtheme signals a moderate level of control. 43% (n=25) of the organisations in the sample did not report on their privacy values. The publication of privacy commitments in a CSR report, without the publication of an organisation's privacy values, could indicate that an organisation associates privacy as a regulatory requirement rather than a societal or stakeholder value that needs to be both articulated and addressed. However it could also suggest that the organisation does not want to publish its values. For instance, studies suggest that organisations with strong brands can often benefit from the lack of transparency in their CSR publications (Allen and Peloza, 2015). Allen and Peloza (2015) suggest that if these organisations were to proactively communicate their CSR values to stakeholders, the brand halo would be tarnished, and the organisation's value would suffer. In either case, both scenarios would still suggest a control-based activity rather than a justice-based one.

Notably, whilst those organisations classified as Food and Beverage did produce CSR reports, they did not report any NMPv activities in their CSR reports. Greenaway et al. (2015) interpret organisations who report minimal, if any, control or justice based privacy activities, to be 'Privacy Ignorers'. However just because an organisation does not report privacy as a nonmarket activity, does not make it a privacy ignorer. Therefore, whilst the

lack of any NMPv activity in a CSR report could have been interpreted as a control score of 3.5 (NoValuesPublished) – there was no content to support such an assertion and so these organisations were not included in the results. Interestingly, the PRC database does not contain any reported breaches for those organisations classified as 'Food and Beverage'. This could be because their product, supply chain and customer engagement simply does not involve the collection or processing of much personal data.

Privacy is Aimed at Internal or External Stakeholders

This code expresses the stakeholder perspectives of Corporate Social Privacy (discussed in Section 2.5). The stakeholder perspective of Corporate Social Privacy assumes that organisations consider the privacy concerns of multiple constituencies including employees, suppliers, consumers, local communities etc. A weighting of '1' was assigned to NMPv activities aimed at internal stakeholders, and NMPv activities aimed at external stakeholders, indicating these activities signal levels of low-control. 51% of organisations *(n=33)* reported NMPv activities aimed at internal stakeholders. Internal stakeholders were typically referred to as the board, employees, contractors, or contingent workers. 49% of organisations (*n=32)* reported NMPv activities aimed at external stakeholders. External stakeholders were typically referred to as suppliers, customers, third parties service providers and developers. When an organisation associated an NMPv activity with internal stakeholder(s), they most often also referenced external stakeholders as well, hence the similarity in the number of reports referencing both internal stakeholders and external stakeholders. For example, in their CSR report, Allstate report NMPv activities associated with external stakeholders:

> *"Allstate emphasizes the importance of customer privacy and data security with suppliers through our procurement standards, practices and contracts. We have established a security assessment program for our suppliers, which includes on-site assessments for critical suppliers. During those assessments, privacy impacts of proposed process changes are evaluated, and privacy issues are opened and tracked*

through remediation. We also require all contingent workers who have access to our network to complete a training course on Allstate's security policies". (Allstate, 2019, p. 27).

Allstate also report NMPv activities associated with internal stakeholders:

"…select employees undergo risk-specific training that addresses topics such as anti-corruption, conflicts of interest, data privacy, equal opportunity, insider trading, procurement, social media, and money laundering". (Allstate, 2019, p. 18).

5.2.4.2 Thematic Analysis: Justice Themes

'Privacy being driven by stakeholder loyalty' was a justice-based subtheme from the Nonmarket Privacy Activities Codebook that was not reported in the CSR reports, i.e., it had a score of zero. This subtheme was removed from the results. The most frequently occurring subthemes for justice were:

- Exceeding regulatory minimums
- C-Suite executive(s) appointed to privacy
- Maximum staff assigned to privacy
- Collaboration with privacy-related and advocacy groups
- Organisation reports their values towards privacy
- Privacy is associated with ethics
- Privacy is associated with stakeholder trust

Examples of the subthemes reported are presented in Table 5.3. These subthemes are discussed in the remainder of this section.

Table 5.3 Examples of Justice Subthemes

Subtheme	Weight	Example	No. Rpts	No. Refs
The organisation advises public policy on privacy.	1	**HP (2019, p. 14):** *"Our privacy and government relations teams work with policymakers to support robust and globally interoperable privacy and data protection regulations".*	11	17
The organisation associate's privacy with brand in corporate publications.	1	**IBM (2019, p. 8):** *"Trust and transparency have always been essential to IBM's success. Today, we consider the impact of our technology on society and accept the responsibility that our digital era demands of innovators. We seek not merely to comply but to lead on the urgent issues of data privacy, ethical AI, inclusiveness in technology design, and more".*	2	3
The organisation associates/funds privacy conferences.	1	**Citi (2019, p. 95):** "*…in 2019 we hosted an event called The Future of Digital Identity that engaged clients, partners, startups and Citi employees. Regardless of the varying perspectives the panelists brought to the event, there was consensus that data privacy and protection are central to advancements in digital identity".*	2	2
The organisation has appointed a privacy representative to the C-Suite.	4.5	**Liberty Mutual (2019, p. 23): "***over the last 12 months, we expanded our Global Privacy Office and appointed a chief privacy office".*	27	43
The organisation's privacy behaviours are driven by stakeholder trust.	4.5	**American Express (2019, p. 22)**: *"We value our customers' trust in our ability to keep their data safe and secure, and we have multiple systems in place to assure customers' data and privacy are protected".*	21	31
The organisation is advice-focused, aiming to build relationships with individuals.	4	**AT&T (2019, p.16):** *"In addition to our actions as a company, we believe one of the best ways to protect privacy is for our customers to follow strong digital security practices. We provide customers with information on how to maintain privacy, safety and security in an increasingly connected world".*	11	18
The organisation develops open standards for privacy.	4	**Google (2019):** *"And we share these technologies with partners and competitors alike, raising industry standards that help keep everyone safer online".*	9	16
The organisation appoints privacy representative to management level.	4	**Merck (2019, p. 28):** *"we have local Data Privacy Officers at various sites around the world".*	6	6
The organisation's privacy behaviours are driven by a code of ethics.	4	**Home Depot (2019, p. 104):** *"Home Depot's ethical and legal standards in these areas: Safety, Labor and employment, Conflicts of interest, Antitrust and fair competition, confidentiality, privacy and information protection".*	22	26
The organisations privacy activities are driven by stakeholder respect.	4	**Google (2019):** *"Respect our users. Respect their privacy".*	11	12
Employee training exceeds regulatory minimums,	4	**Cisco (2019, p. 112):** *"We include data privacy and security topics in our Code of Business Conduct. And we offer more than 100 hours of additional training content for anyone who is interested or whose job requires enhanced expertise".*	18	23
The organisation operates as a steward of information.	4	**Verizon (2019, p. 43):** *Section Headline :* "*Our stewardship of personal data".*	1	1
The organisation lobbies governments	4	**AT&T (2019, p. 16):** *"AT&T advocates for the adoption of U.S. federal consumer privacy legislation ensuring a unified*	1	1

Subtheme	Weight	Example	No. Rpts	No. Refs
for privacy standards that are most beneficial to their consumer.		*approach to privacy, data security and breach notification that is consistent with Federal Trade Commission standards".*		
Ownership is shared between the individual and organisation, however the individual expresses greater ownership.	4	**Google (2019):** *"you're in control. We know that one size doesn't fit all when it comes to privacy, so we build powerful, easy-to-use privacy tools into your Google account. They give you control over the privacy settings that are right for you, and what types of data we collect and use across our services".*	7	14
The organisation publishes their values towards privacy in corporate publications.	4	**Microsoft (2019, p. 6):** *"We ground our privacy commitments in strong data governance practices, so you can trust that we'll protect the privacy and confidentiality of your data and will only use it in a way that's consistent with the reasons you provided it".*	37	74
Strategic collaboration with privacy advocacy groups.	5	**Dell (2019, p. 40):** *"We conducted a demo of the tool for EU privacy regulators, who had very positive feedback. This collaboration was highlighted at a Dell Technology World booth, where our privacy team and RSA representatives talked to customers. Dell Technologies' Privacy Office also held one-on-one best practice-sharing dialogues with our customers' privacy officers".*	24	46
The organisation exceeds regulatory privacy minimums.	5	**Apple (2019, p. 21):** *"Apple maintains current ISO 27001 and ISO 27018 certifications. Apple undergoes yearly re-audits in order to receive these certifications. We also use techniques like Differential Privacy to improve user experiences while protecting the information you share with Apple".*	44	135
The organisation lobbies governments for privacy standards more beneficial to society than to organisation.	5	**IBM (2019, p. 12):** "*IBM has called for a precision regulation approach to addressing Americans' privacy concerns and has actively encouraged the U.S. Congress and governments worldwide to make privacy protections a priority".*	3	4
Privacy is linked to stakeholders.	5	**Ford (2020, p. 52):** *"Trust is about managing risk and uncertainty, and our Trust Framework is built on honesty, expertise and care. We need to display these now, in the near future and over the long term to build trust. The critical enabler is giving customers, suppliers and other stakeholders relevant information to be transparent and open – but always with data privacy and safety in mind".*	15	23
Stakeholders value privacy.	5	**Citi Group (2019, p. 93):** *"Data security and privacy are top priorities for Citi and for our stakeholders and are among our most material ESG issues".*	4	8

Exceeding Regulatory Minimums

The SMEs assigned a weighting of '5' to an NMPv activity that exceeds regulatory minimums i.e., an NMPv activity that goes beyond mere compliance. A weighting of 5 indicates this subtheme signals very high levels of justice. An organisation might, for instance, report an NMPv activity that privacy legislation does not currently prescribe, such as a CEO authoring a book on the importance of digital privacy, or developing open standards for privacy. Or an organisation may report exceeding requirements already prescribed in legislation. For instance, where legislation such as CCPA and GDPR may mandate appropriate training of all employees handling personal information, an organisation might report exceeding this by training more stakeholders than they are legally obliged to, for example, by providing training to all employees regardless of their role, or by providing training for suppliers and third parties rather than rely solely on data protection agreements, or by providing training for customers. In this study, 68% of organisations reported NMPv activities exceeding regulatory minimums *(n=44*), and 34% of organisations reported NMPv activities exceeding minimum employee training requirements *(n=22)*. Some organisations reported that they exceed regulation, but do not outline how. HP, for example, report:

> *"we focus on providing protections that exceed legal minimums and on deploying consistent, rigorous policies and procedures, giving people confidence when sharing information with us and using our products" (HP, 2019, p. 28).*

Other less common types of NMPv activities reported that exceeded privacy regulation are listed in Table 5.4, together with examples of how the activity is reported in the CSR reports and an explanation of how that activity exceeds regulation.

Table 5.4 How NMPv Activities Exceeding Regulation are Reported

Exceeding regulation	How the activity is reported	How the activity exceeds regulation
Using systems/tools to enhance privacy.	**Apple (2019):** *"Safari is the first browser to offer DuckDuckGo as a built-in option that you can set as your default search engine, which allows you to search the web without being tracked."*	There is currently no legislation (in Europe or the US) stating that an organisation **must** provide the ability to not be tracked. Tracking must be clearly outlined in the privacy statement or notice, and requires consent.
Publication (book or white paper) by senior executives on privacy.	**Microsoft (2019, p. 7):** "*…a new book by Microsoft President Brad Smith and Microsoft Senior Director of External Relations and Executive Communications Carol Ann Browne, discuss the impact of AI, the rise of cyberattacks, threats to digital privacy".*	There is no legislation stating that an organisation's senior leadership must author a book that includes privacy issues.
Offering legislative requirements even where not mandated	**Apple (2019):** *"At Apple we design our products and services according to the principle of privacy by default and collect only the minimum amount of data necessary to provide our users with a product or service."*	Whilst Privacy by Design and data minimisation are principles of GDPR and CCPA, Apple is not obligated to offer CCPA or GDPR compliance to all its clients.
Development of industry standards.	**IBM (2019, p. 13):** "*IBM was an early leader in developing (and adopting) the EU Data Protection Code of Conduct for Cloud Service Providers"*	Whilst it might be beneficial for an organisation to develop standards where none exist and to make those standards available publicly for other organisations to adopt, it is not legally mandatory.
Development of industry surveys/benchmark studies.	**Cisco (2019, p. 111):***"highlighted the business value of good data privacy with the Cisco 2019 Data Privacy Benchmark Study. The survey was completed by thousands of security professionals worldwide. It revealed the financial benefits of good data privacy processes, including shorter delays in sales cycles. The study was downloaded about 3,500 times".*	There are no regulatory requirements to produce industry reports or surveys.
Commitment to a voluntary set of privacy related industry standards.	**General Motors (2019, p. 78):**_*"….continues to be committed to the Auto Alliance Consumer Protection Privacy Principles for Connected Vehicles".*	The Consumer Privacy Protection Principles for Vehicle Technologies and Services provide guidelines to ensure baseline customer privacy when it comes to vehicle technologies and services. The Principles build on FIPPs, FTC guidance, and the Consumer Privacy Bill of Rights to deliver updated protections for the personal information of vehicle owners. However the principles are discretionary and not mandated.
	Oracle (2019, p. 9):*"Earned a Privacy Mark accreditation from the Japan*	The grant of use of PrivacyMark requires third-party organisations to objectively evaluate the compliance of organisations with all relevant

Exceeding regulation	How the activity is reported	How the activity exceeds regulation
	Institute for Promotion of Digital Economy and Community".	laws, standards and regulations, and allows organisations to demonstrate that they are in compliance with the law and that they have voluntarily established a personal information protection management system with a high level of protection. There is no requirement in legislation to mandate the implementation of the PrivacyMark.
	Verizon (2019, p. 47): *"was one of the original signatories to the GSMA Digital Declaration, launched in 2019, which calls on businesses to respect the privacy of digital citizens, handle personal data securely and transparently, take meaningful steps to mitigate cyber threats…".*	Whilst these principles may appear similar to those enshrined in GDPR and CCPA, neither CCPA nor GDPR are applicable to all Verizon customers, and therefore handling of personal data securely and transparently may be discretionary in many cases.
Funding of privacy initiatives.	**Disney (2019, p. 24):** "*we recognize that we have an opportunity to support children and caregivers as they navigate their own digital environments. Our Digital Citizenship grants support nongovernmental organisations and are designed to promote, enhance, and expand children's digital wellbeing. Grantees in this portfolio provide expertise in areas including digital literacy and resilience, privacy, critical thinking, and educator training and curriculum*".	Whilst there are several privacy laws in the US, there are none that mandate the provision of funding for NGOs for digital (privacy) wellbeing.
Training stakeholder beyond regulatory minimums.	**AT&T (2019, p. 16):** *"We provide customers with information on how to maintain privacy, safety and security in an increasingly connected world".* **Disney:** "*In 2019, Disney funded initiatives that supported awareness-raising tips and tools for parents; educator trainings; curriculum about basic privacy skills, fake news, and safe searches; and chat lines and hotlines working with children in crisis".*	Several privacy regulations outline the requirement to provide training to employees who handle personal information. However some organisations exceed the prescribed level of training and/or train external customers, associates and/or suppliers whilst not being legally mandated to do so.
Calling for enhanced/additional laws regarding privacy.	**Cisco (2019, p. 11):** *"In FY19, our CEO Chuck Robbins called for comprehensive laws that respect privacy as a fundamental human right…".*	Whilst the CSR reports in the sample often refer to Privacy, they refer to privacy as Data Protection/Data Privacy, rather than Privacy as a Human Right. Pursuing privacy as a Human Right extends privacy beyond Data Protection.

Responsibility for Privacy is Appointed to C-Suite Level

The SMEs assigned a weighting of '4.5' to assigning responsibility for privacy to the most senior management positions or the C-Suite. These weightings indicate that this subtheme signals very high levels of justice. The appointment of a privacy representative to the C-Suite is an NMPv activity which exceeds regulatory minimums. There is no legislation that mandates the appointment of a Chief Privacy Officer or to establish privacy councils or senior privacy risk oversight committees, therefore this NMPv activity also exceeds regulatory minimums. 41% of organisations *(n=27)* in the sample reported having a senior C-Suite representative(s) for privacy. Notably, almost all the organisations classified as Technology *(n=7)*, reported privacy at the C-suite level. Senior roles were most often referred to as a Chief Privacy Officer, Chief Trust Officer or a Chief Risk and Compliance Officer. These roles were typically part of a senior leadership team or risk committee. For example, IBM reports:

> *"IBM was among the first companies to appoint a chief privacy officer (in 2000)." (IBM, 2019, p. 13).*
>
> *And*
>
> *"we ….created a Senior-VP-level Privacy Advisory Committee and by expanding the mission of our Chief Privacy Office, which is deeply integrated with our cybersecurity and data functions, and with each IBM business unit." (IBM, 2019, p.13).*

It would seem reasonable to suggest that this activity is one which would indicate that the organisation takes privacy seriously, and that privacy matters to them and their reputation. However, it is also notable that many organisations in the sample are in regulated industries such as Financial Services, Pharmaceuticals, Telecommunications and Transport sectors. In these sectors, governance and oversight of risk is of high importance for continued operations, and responsibility to ensure privacy risk is managed proactively and is assigned to senior management. Table 5.5 summarises this theme across the dataset,

using the industry categorisation from the Fortune 100 index (see Appendix H for a breakdown of the sample of organisations by this industry categorisation).

Table 5.5 Organisations Who Appointed Responsibility for Privacy to Senior or C-Suite Executive(s)

Industry	***Organisation***
Technology	Cisco
	HP
	IBM
	Microsoft
	Apple
Telecommunications	Verizon
	AT&T
Financial	Allstate
	Citi
	Anthem
	Liberty Mutual
	Nationwide
	Prudential
	Wells Fargo
Food and Drug Stores	Kroger
Healthcare	Anthem
	Cardinal Health
	Cigna
	CVS Health
	Merck
	United Health
Retailing	Lowes
	Home Depot
Transport	American Airlines
Energy	ConocoPhillips
Industrials	Deere
Oil and Gas Equipment	Enterprise Partners

The SMEs assigned a weighting of '4' to appointing responsibility for privacy to a middle management position. This weighting indicates that this subtheme suggests high levels of justice, but less justice than appointing privacy responsibility at C-Suite level. Data Protection Managers, who are typically positioned in middle management, were most often

referred to as a Data Privacy Officer, Data Protection Officer or Data Privacy Manager. Ingram Micro for example, reported:

> *"A data privacy officer oversees our privacy program and ensures that we embed privacy by design into our projects". (Ingram Micro, 2018, p. 80).*

Six organisations in the sample reported having a Data Protection Manager appointed, namely; Best Buy, Cigna, GE, HP, Ingram Micro and Merck.

Collaborations with Privacy and Advocacy Groups

When organisations collaborate with other organisations with regard to privacy, this demonstrates the strategic perspective of Corporate Social Privacy, outlined in Section 2.5. Strategic perspectives of Corporate Social Privacy are driven by organisational concerns about generating value from market-based solutions that address privacy in a socially responsible way. The SMEs assigned a weighting of '5' to NMPv collaborations with privacy groups and advocacy groups. These weightings indicate that this subtheme suggests very high levels of justice. 35% of organisations in the sample *(n=23)* reported NMPv-related collaborations. All but one of the organisations in the sample that were classified as Technology *(n=8)* reported these types of collaborations (Oracle did not), as did two of the organisations in the sample classified as Telecommunications. Whilst few organisations reported the aims of their collaborations, AT&T report:

> *"We believe that industry collaboration is an important way to reach agreement on the principles that should form the foundation of consumer privacy law" (AT&T, 2019, p. 16).*

There was a vast range of collaborations reported, which we have categorised in the following ways:

- membership of professional groups such as the International Association of Privacy Professionals (IAPP);
- engaging with governments and councils on privacy standards, such as the EU Privacy Shield (since invalidated);
- participating in advocacy groups to collectively lobby or champion privacy changes e.g., The Future of Privacy Forum or The Centre for Information Policy Leadership;
- partnering with bodies such as the International Standards Organisation (ISO) to develop or enhance privacy related principles or standards;
- partnering with other industries or organisations to provide enhanced privacy services, products, or events to customers or the wider stakeholder community.

The Organisation's Privacy Values are Reported

The SMEs assigned a weighting of '4' to the publication of values regarding privacy. These weightings indicate that this subtheme signals high levels of justice. 37 organisations in the sample published 74 privacy values. When an organisation reports privacy values, it can often be difficult to determine if an organisation is merely reporting these values to appease stakeholders (Kolk, 2003), or to 'look good rather than be good' (Chun et al., 2019). Notwithstanding this, corporate self-reports (such as CSR reports), typically signal values that an organisation perceives as important to them (Gibson and Guthrie, 1996). Furthermore, what organisations choose to include in, and omit from, their corporate reports, is a conscious decision that communicates a significant message to stakeholders. There were many different types of values reported in the data set, and they are summarised here into five categories:

- Statements of belief towards privacy, where. reporting typically begins with 'we believe…', 'we feel…', 'we recognise…', 'it is our belief…' etc. For instance, United Health report that:

"We believe health care data and related information should only be used solely for the purposes of improving individual health, advancing health system performance and to aid in new discovery". (United Health, 2019, p. 28).

- Commitments towards privacy, where reporting typically begins with 'we never…, 'we always…' etc. For instance, Google report that:

  " we never sell our users' personal information to anyone….it's important to clarify that our users' personal information is simply not for sale". (Google, 2019).

- Aspirations towards privacy, where reporting typically begins with 'we seek…', 'we try…', 'we expect….', 'we hope…' etc. For instance, IBM report that:

  "We seek not merely to comply but to lead on the urgent issues of data privacy, ethical AI, inclusiveness in technology design, and more.(IBM, 2019, p. 8).

- Importance of privacy to the organisation. For instance, Cigna report that:

  "Protecting the privacy of our customers, employer clients, employees, and business partners is of the utmost importance to us". (Cigna, 2019, p. 15).

- Privacy as an activism value. In the shared value perspective of Corporate Social Privacy, privacy activism emerges. This type of value was reported only by Apple, Cisco, Microsoft, AT&T, Microsoft and Verizon. For instance, Cisco report that:

  "In FY19, Cisco CEO Chuck Robbins called for U.S. federal data protection legislation that recognizes privacy as a human right. (Cisco, 2019, p. 106).

The Organisation Reports that Privacy is Driven By Stakeholder Trust

The SMEs assigned a weighting of '4.5' to NMPv activities associated with stakeholder trust. This weighting indicates that this subtheme signals high levels of justice. This code was interpreted to mean where an organisation associates or shapes a privacy activity as one that nurtures or sustains the consumer trust relationship. So, whilst American Express reported trust and privacy together, they did not frame privacy as being driven by consumer trust:

> *"We value our customers' trust in our ability to keep their data safe and secure, and we have multiple systems in place to assure customers' data and privacy are protected." (American Express, 2019, p. 22).*

In this way, 33% of organisations *(n=21)* reported that privacy was driven by stakeholder trust. With the exception of Apple, the organisations in the Warrior and Citizenship NMPv orientation (*n=7*) reported this subtheme. For example, HP report:

> *"HP recognizes the fundamental importance of privacy, security, and data protection to our employees, customers, and partners worldwide. This commitment is a critical pillar of brand trust and increasingly a source of competitive advantage in an era of accelerated innovation, global data proliferation, and fast-changing regulatory frameworks." (HP, 2019, p. 30).*

Several (*n=11*) of the organisations who reported privacy being driven by stakeholder trust, also included the term 'respect', for example, Cigna report:

> *"At Cigna, we respect our customers' and clients' right to privacy and value the trust they place in us". (Cigna, 2019, p. 15).*

Similarly, Google report:

> *"Respecting the privacy of our users means protecting the data that they trust us with". (Google, 2019).*

The Organisation Reports that Privacy is Associated With A Code Of Ethics

The SMEs assigned a weighting of '4' to an NMPv activity that is associated with a code of ethics. A weighting of 4 indicates this subtheme signals a high level of justice. 34% of organisations *(n=22)* report that a code of ethics played a role in their privacy programs. For example, Dell report:

> *"Our vision for 2030 articulates how we will focus on creating a positive social impact in three key areas: Advancing Sustainability, Cultivating Inclusion and Transforming Lives with Technology. Underlying all of this is our strong commitment to ethics and privacy." (Dell, 2019, p. 57).*

Notably, the organisations in the sample that were categorised as healthcare and referenced privacy *(n=13)*, also associated privacy with ethics.

5.2.4.3 Thematic Matrix Analysis: NMPv Orientations

The final part of the thematic analysis was the production of the coding matrix, as described by Groenland (2018). This matrix provides the tallies that enable an organisation's NMPv orientation to be determined. NVivo recorded the 'tallies' for each subtheme recorded in each CSR report. A coding matrix was produced using NVivo's 'produce matrix' option, and results were imported into Excel. The 'tallies' for each subtheme were then weighted by multiplying them by the weightings outlined for each subtheme in the Nonmarket Privacy Activities Codebook. The resulting totals for each organisation's CSR report can be found in Appendix O. These results are then plotted on a scatter chart using Microsoft Excel's chart function, as presented in Figure 5.2. After plotting the scatter chart in this way, the four distinct NMPv orientations emerge in terms of control and justice. In this way, the research responds to RQ2: *Can an organisation's approach to NMPv be determined from their published NMPv activities?* The research also responds to calls from Greenaway et al. (2015) to construct a mechanism that can determine an organisation's privacy orientation, as characterised by levels of control and justice in their reported privacy activities. Whilst the resulting orientations are no doubt skewed, this likely reflects that most organisations approach privacy as a compliance requirement, similar to findings from Pollach (2011). For instance, for organisations in the Risk Management NMPv orientation, privacy is often a 'mention' rather than a full section of a CSR report.

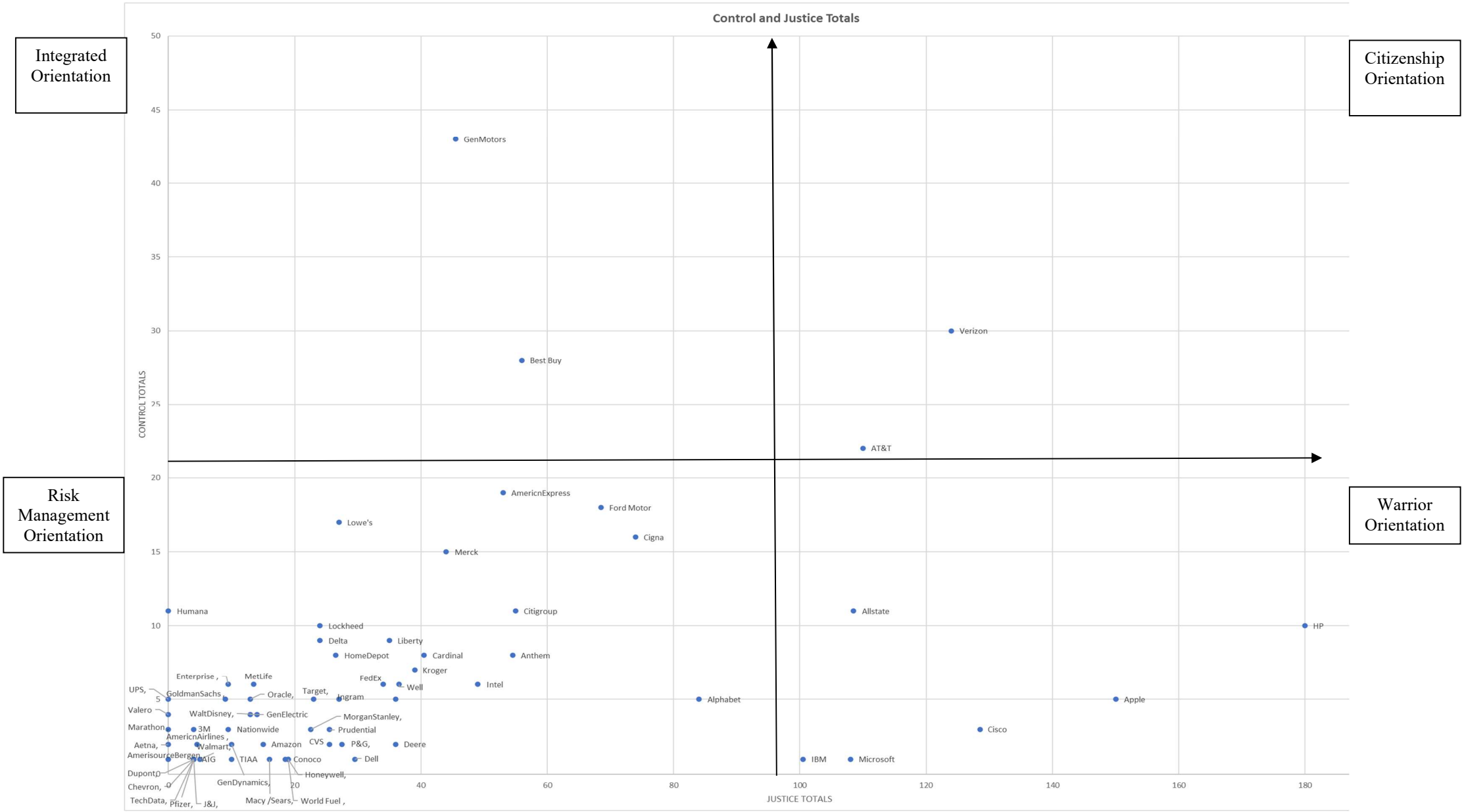


Figure 5.2 Results for the Nonmarket Privacy Orientations Matrix

To illustrate each NMPv orientation, an exemplar organisation for each NMPv orientation was selected. The CSR report from the exemplar organisation needed to contain sufficient privacy activities to discuss its NMPv orientation. Two criteria were applied to select exemplar organisations. First, their CSR report had to be aligned to a structured CSR reporting framework, such as the Global Reporting Initiative (GRI), as this would establish a minimum level of content. Second, the CSR report had to contain a materiality assessment section, as this would provide insight into the views of key stakeholders and the organisation toward privacy. A materiality assessment is the process of identifying, refining, and assessing numerous potential environmental, social and governance issues that matter most to an organisation and its key stakeholders, and condensing them into a shortlist of topics that inform organisational strategy, targets, and reporting (Global Reporting Initiative, 2016). Over 80% of the world's largest 250 companies include materiality assessments in their CSR reports (KPMG, 2013).

Almost half of the reports that referenced privacy in this study (*n=32*) reported having undertaken a materiality assessment, and included the results in their CSR report. Notably, the first reference to privacy in many of the CSR reports, was in their materiality assessment section. For this reason, when discussing the exemplar organisation's CSR report, their materiality assessment is also presented. Ingram Micro was selected to represent the Risk Management NMPv orientation. BestBuy was selected to represent the Integrated NMPv orientation. Verizon was selected to represent the Citizenship NMPv orientation. Cisco was selected to represent the Warrior NMPv orientation.

The Risk Management NMPv Orientation (Low Control–Low Justice)

Unsurprisingly, the Risk Management NMPv orientation represents the most common orientation (*n*=55). This orientation is characterised by evidence of control-based activities that are focused on simple compliance. Organisations situated in this orientation report privacy as a compliance requirement and report limited NMPv activity exceeding regulatory minimums. Whilst 25% of organisations *(n=15)* in this orientation reported collaborations, they collaborated in a way that benefitted themselves or immediate stakeholders. For example, Goldman Sachs reported:

> *"We partnered with Apple to launch a no-fee credit card that incorporates new levels of privacy, security and transparency, and provides tools that make it easy to …for customers how to save on interest". (Goldman Sachs, 2019, p. 23).*

Lobbying for privacy measures that are more beneficial to the organisation, is evidence of a Risk Management NMPv orientation. However, no organisations situated in this orientation reported this activity. Indeed, it was only reported by HP, who are positioned in the Warrior NMPv orientation. The limitation of using only CSR reports, is that an activity such as lobbying may in fact be conducted by an organisation, however, not reported in their CSR report. For instance, Google (Alphabet), situated in the Risk Management NMPv orientation did not report lobbying in their CSR report, however they have lobbied for privacy that is more favourable to itself than consumers (New York Times, 2021).

Organisations in the sample that are categorised as healthcare, travel and financial services are situated in this orientation. This may be related to the extent of regulation in these sectors. In highly regulated industries, compliance with regulation is important for operational and financial sustainability. Ingram Micro's CSR report is discussed as an exemplar of the Risk Management NMPv orientation below.

Risk Management NMPv Orientation Exemplar

Ingram Micro is classified in the Wholesale Industry by the Fortune index. Primarily, it is a B2B business, offering cloud distribution of applications (technology and supply chain services) to other businesses, via a centralised digital distribution channel. Ingram Micro represents over 1,600 suppliers, including Acer, Apple, Cisco, Citrix, HP, IBM, Lenovo, Microsoft, Samsung, Symantec, and VMware, and more than 170,000 customers in approximately 160 countries (Ingram Micro, 2021). Whilst Ingram Micro process significant amounts of employee personal data, personal data is not central to their business or their operations.

The Nonmarket Privacy Orientation Matrix asserts that organisations situated in this orientation signal low levels of control, and low levels of justice. Ingram Micro's materiality assessment, as outlined in Figure 5.3, shows privacy to be of moderate importance to stakeholders, whilst having a high impact on Ingram Micro.

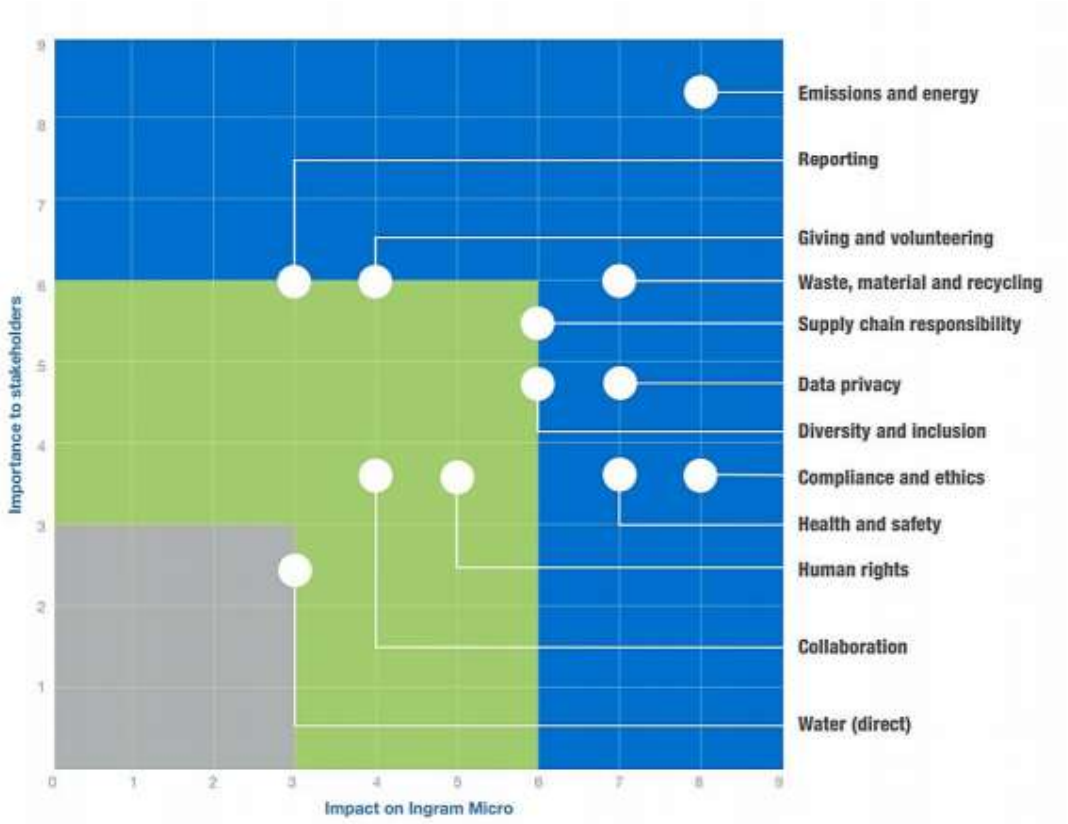


Figure 5.3 Ingram Micro Materiality Assessment (Ingram Micro, 2018, p.16)

Notably ‘compliance’ is reported to be considered by stakeholders to have lesser importance than privacy, and is positioned as moderately important to stakeholders. On the other hand, ‘compliance’ is positioned similarly to ‘data privacy’, and both are positioned at ‘7’. Where stakeholders do not value compliance, less control can be signalled by an organisation. In this way, it would appear that Ingram Micro is situated in a NMPv orientation that reflects its stakeholders needs, together with Ingram Micro’s own requirements.

Signaling low levels of control, Ingram Micro report NMPv activity as a simple compliance issue:

> *“We manage anti-corruption as part of a broader, formal compliance effort that includes data privacy, anti-bribery, conflict of interest, trade controls, anti-money laundering, gray market, antitrust risk, harassment and whistleblower compliance” (Ingram Micro, 2018, p.25).*

Signaling low levels of justice, Ingram Micro does not relate business strategy, vision or mission to any NMPv activities, nor do they report privacy values or report collaborations with privacy advocacy groups. Ingram Micro report that responsibility for privacy is assigned to a middle management position:

> *“A data privacy officer oversees our privacy program and ensures that we embed privacy by design into our projects.” (Ingram Micro, 2018, p.25).*

This pattern of reporting would indicate a low justice orientation.

The Integrated NMPv Orientation (High Control–Low Justice)

The Integrated NMPv orientation is characterised by evidence of high levels of control-based NMPv activities. Two organisations are positioned in the Integrated NMPv orientation; Best Buy and General Motors. Although justice-based NMPv activities are limited, organisations in this orientation report the privacy needs of the wider stakeholder community, beyond customers, shareholders and governments. Such wider stakeholder groups may include other industries, non-customers and society. In this way, organisations situated in the Integrated NMPv orientation may report stakeholder perspectives of NMPv. However, unlike the Risk Management NMPv orientation, organisations in the Integrated NMPv orientation may express robust compliance to regulation as a baseline, but may also express activities beyond compliance. For example, whilst 58% of the organisations positioned in the Risk Management NMPv orientation (*n*=32) reported evidence of NMPv activities that exceeded regulatory minimums, all of the organisations positioned in the Integrated, Citizenship and Warrior NMPv orientations (*n=10),* reported evidence of NMPv activities exceeding regulatory minimums. For instance, General Motors report:

> *"Our contracts lay out expectations for lawful compliance with data protection and privacy laws and regulations. In addition, our Board of Directors has approved the adoption of Global Privacy Principles, and GM continues to be committed to the Auto Alliance Consumer Protection Privacy Principles for Connected Vehicles." (General Motors, 2019, p. 78).*

The adherence to the 'Auto Alliance Consumer Protection Privacy Principles'[5] is an industry-led, rather than legislatively-led initiative, and is as such discretionary. Whilst one could argue that organisations must engage with such initiatives in order to maintain competitive parity, it is still not obligatory. In this orientation, organisations report privacy as a value, rather than simply a compliance requirement. Over half (*n=28*) of the organisations positioned in the Risk Management NMPv orientation reported no evidence

[5] A set of voluntary privacy principles developed by the Alliance of Automobile Manufacturers *https://knowledgecenter.csg.org/kc/system/files/CSG%20AV%20Lunch%20presentations.pdf*

of privacy values, whereas the organisations in the Integrated, Citizenship and Warrior NMPv orientations (*n=10*) report evidence of these values. In this orientation, investment in privacy is also reported. For instance, General Motors reports:

> *"The Privacy Office has a privacy program framework that focuses on policies, procedures, tools, guidance and training. This framework also includes a Privacy-by-Design program that requires all data-dependent initiatives to receive a privacy-focused consultation through its life cycle. The privacy program and office reside with our legal staff, and additional non-legal resources are leveraged on a functional, regional and product/program basis to instill best practices across the enterprise.." (General Motors, 2019, p. 78).*

It is important to highlight however, that 'Privacy-By-Design' referenced above by General Motors, is enshrined in the GDPR. Therefore, it is difficult to determine from their CSR report if General Motors is obligated by GDPR. Best Buy's CSR report is discussed below, as an exemplar of the Integrated NMPv orientation.

Integrated NMPv Orientation Exemplar

Best Buy, classified by the Fortune index in the Retail industry, is a provider of consumer technology products and services, offering a range of merchandise and services to customers, including consumer electronics, appliances, computing devices, mobile phones, entertainment, and other products. Its services include consultation, delivery, design, health-related services, installation, memberships, repair, set-up, technical support, and warranty-related services [6]. Whilst Best Buy does not rely on personal data for its business model, Best Buy processes a high number of customer transactions, including cardholder data (Experian, 2001). In this way, Best Buy would need to have strong controls in place to protect their consumer personal data. Best Buy's materiality assessment, as outlined in Figure 5.4, reported that 'Data Privacy of Connected Devices' was a differentiator that is really important to their stakeholders, and has a significant impact on Best Buy's business.

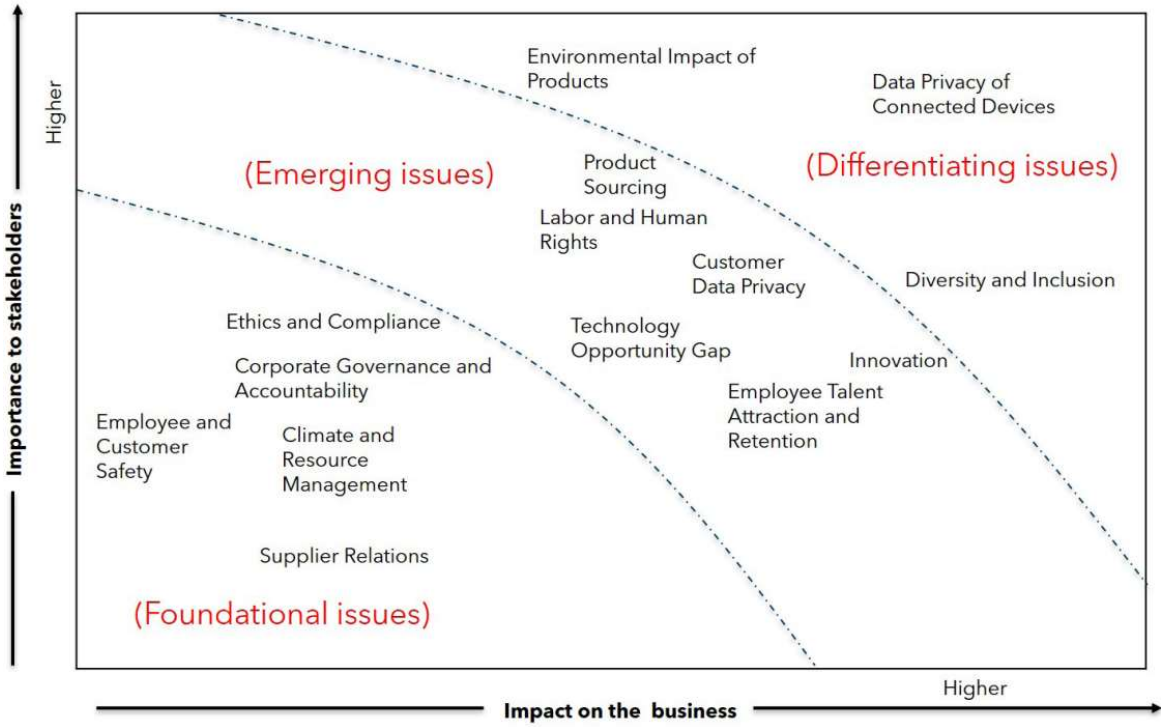


Figure 5.4 Best Buy Materiality Assessment (Best Buy, 2019, p. 8).

[6] https://www.reuters.com/companies/BBY.N

'Customer Data Privacy' is classified in their materiality assessment as an emerging issue, that again is of high importance to both the customer and the organisation. However, 'Customer Data Privacy' is positioned in their materiality assessment with lesser importance to 'Data Privacy of Connected Devices', which is classified as a differentiating issue. In this way, Best Buy recognises the business value that privacy has to offer in the future of connected devices.

Best Buy offers reports evidence of compliance with regulation, specifically the Health Insurance Portability and Accountability Act:

> *"We require all persons who access, use, or disclose protected health information to be properly trained about HIPAA in order to comply with all state and federal laws for safeguarding individually identifiable health information". (Best Buy, 2019, p. 8).*

Best Buy also classifies compliance as a 'foundational issue' in their materiality assessment, In this way, this pattern indicates a high-control orientation. Organisations in the Integrated NMPv orientation are awake to the need for collaboration with stakeholders beyond their customers, and to understand more fully what the privacy 'norms' are in their industry, rather than just privacy laws themselves. For instance, Best Buy report:

> *"Best Buy is a corporate member of the International Association of Privacy Professionals….of the Association of Corporate Counsel (ACC)…..an active participant in ACC's Information Technology, Privacy and eCommerce Committee….the RILA Privacy Leaders Council. These memberships help us understand industry shifts, benchmark our peers to help maintain appropriate privacy and security standards, and provide input as a retail industry on privacy legislation or other regulatory requirements that will impact our business…" (Best Buy, 2019, p. 37).*

Notwithstanding this, Best Buy also report that their focus remains on legal privacy requirements 'impacting our business' which would indicate a tendency towards a low-justice orientation. Organisations in the Integrated NMPv orientation are aware of the

importance of stakeholders beyond themselves, and Best Buy extends the reach of their NMPv activities to the wider stakeholder community, for example:

> *" As smart home growth continues to expand…we strive to address privacy concerns directly and give consumers control over their personal data. We are achieving this through partnering with industry work groups …. and working to establish a customer baseline of expectations in the area of security and privacy with respect to IoT devices. Numerous public and private entities are developing testable standards in this space that we believe could be adapted for scalable deployment. This will enable …. manufacturers, retailers, and service providers to make consistent representations to customers regarding the security and privacy attributes of the IoT devices they offer". (Best Buy, 2019, p. 38).*

Organisations in the Integrated NMPv orientation also frame privacy beyond being only a data protection or data privacy right, to being a human right. Reflecting this, Best Buy reported:

> *"Our Human Rights Policy is the basis of our management system and focuses on the following stakeholders….., including their right to privacy.." (Best Buy, 2019, p. 35).*

The Citizenship NMPv Orientation (High Justice-High Control):

The Citizenship NMPv orientation is one that is characterised by evidence of high levels of control-based NMPv activities and high levels of justice-based NMPv activities. In the Citizenship NMPv orientation, political perspectives, shared value perspectives and strategic perspectives of Corporate Social Privacy are present in CSR reports. Additionally, perspectives of CPA, in the form of lobbying for privacy that favours the consumer or society, are also evident. Both Warrior and Citizenship NMPv orientations consider privacy to be strategic. Privacy activities are focused on building and maintaining sustainable relationships, and often exceed compliance obligations.

A theme consistent across the organisations positioned in both of the high-justice NMPv orientations i.e., Warrior and Citizenship, and found in all their CSR reports, was that these organisations had all appointed a C-Suite executive(s), or C-Suite committee, responsible for privacy. In this way, it would seem that organisations in the high-justice orientations consider privacy to be an issue requiring senior leadership and senior management oversight. Interestingly, all the organisations in the Warrior (*n=6*) and Citizenship (*n=2*) NMPv orientations reported on not just one individual role, but privacy committees or privacy offices at senior management level. For example, IBM report:

> *"we further strengthened our commitment to IBM's established principles for trust and transparency by creating a Senior-VP-level Privacy Advisory Committee and by expanding the mission of our Chief Privacy Office, which is deeply integrated with our cybersecurity and data functions, and with each IBM business unit." (IBM, 2019, p. 13).*

Verizon's CSR report is next discussed, as an exemplar of the Citizenship NMPv Orientation below.

Citizenship NMPv Orientation Exemplar

Verizon, classified by the Fortune index in the Telecommunications industry, provides communications, information and entertainment products and services to consumers, businesses and governmental agencies. Its Consumer segment provides wireless and wireline communications services. In 2020, Verizon Wireless had almost 94m subscribers (Statistica, 2021). Its Business segment provides wireless and wireline communications services and products, including data, video and conferencing services, security and managed network services, local and long-distance voice services and network access to deliver various Internet of Things services and products[7]. In this way, Verizon hosts, transfers and processes huge quantities of personal data.

Verizon reports NMPv activities that measure high on justice and high on control, and is thus positioned in the Citizenship NMPv orientation. In Verizon's materiality assessment, as outlined in Figure 5.5, privacy is positioned with a high impact on society and a high impact on the business. Interestingly, the Y axis title in Verizon's materiality assessment refers to the impact on 'society', rather than 'stakeholders'

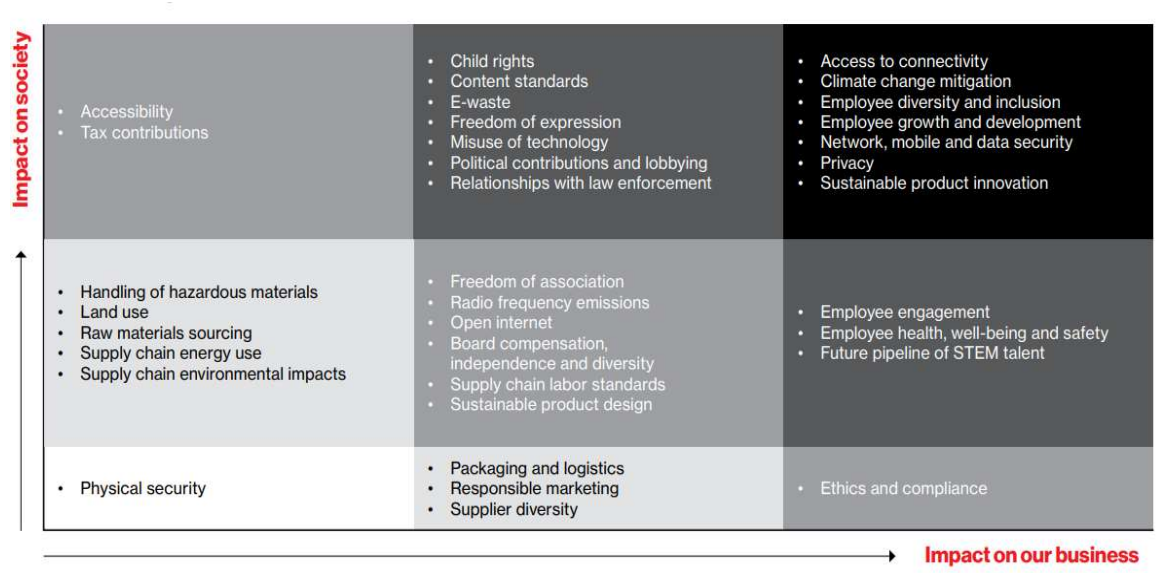


Figure 5.5 Verizon Materiality Assessment (Verizon, 2019, p. 11)

[7] https://www.reuters.com/companies/VZ.N

Thus, in this orientation, organisations position privacy as a societal concern rather than just an individual stakeholder concern. In the Verizon CSR report, their CEO comments:

> *"At the heart of Verizon 2.0 is a commitment to consider how our company interacts with all our stakeholders, including customers and shareholders, as well as our employees, our ecosystem of suppliers and society overall" (Verizon, 2019, p. 3).*

Ethics and Compliance are reported in their materiality assessment to have a high impact on the organisation. This is in contrast to the materiality assessments in previous orientations, where compliance was positioned as moderately impactful/important. Notably, ethics and compliance are combined as one item in the materiality assessment.

For organisations in the Citizenship NMPv orientation, responsibility for privacy is positioned at senior level:

> *"Our work in this area is conducted under the oversight of our Chief Privacy Officer, who reviews and discusses data privacy risks and mitigating actions with the Audit Committee of our Board of Directors"(Verizon, 2019, p. 42).*

This orientation also expresses many of the privacy activities associated with more recent perspectives of NMPv such as creating shared value, strategic and political NMPv. For example, Verizon reported that the protection of privacy is strategically associated with growing the business:

> *"We recognise that protecting data privacy is fundamental to maintaining the trust of our customers and growing our business" (Verizon, 2019, p. 42).*

Verizon also reported the shared value perspectives of NMPv, by reporting on the provision of privacy-enhanced services to customers that would benefit both them and their customers:

> *"Verizon Media launched OneSearch, a search service with enhanced privacy features that gives unbiased and unfiltered results. Additional OneSearch features include : No cookie tracking, retargeting or personal profiling; No sharing of*

personal data with advertisers; No storing of user search history ;Encrypted search terms. (Verizon, 2019, p. 47).

In addition to OneSearch, Verizon also reported the production of the Verizon Data Breach Investigations Report (a highly reputable and annually produced report of data breaches across all sectors). Verizon reported that the driver for the production of the Verizon Data Breach Report is to :

"help our customers better understand the cybersecurity threats they may face and how to manage these risks effectively" (Verizon, 2019, p. 49).

There is also evidence of the political perspective of NMPv in Verizon's CSR report:

"We continue to advocate for a uniform federal privacy framework that can apply to all players in the digital technology ecosystem and make clear, consistent rules of the road for everyone so that our customers' trust and privacy come first—no matter how they use their devices, apps or services" (Verizon, 2019, p. 47).

Interestingly, Verizon was the only organisation in the entire sample to specifically mention the term 'Information Stewardship,' a high-justice theme. They dedicate an entire section of their CSR report to the subject. Organisations in the Warrior (*n=5*), Integrated *(n=2*), and Citizenship (*n=2*) NMPv orientations reported collaborations. Allstate was the only organisation in the Warrior NMPv orientation who did not. Citizens and Warriors were collaborating with organisations in a way that benefitted, not just the organisation, but also the wider stakeholder community or society. For example, Verizon reported:

"Verizon was one of the original signatories to the GSMA Digital Declaration, launched in 2019, which calls on businesses to respect the privacy of digital citizens, handle personal data securely and transparently, take meaningful steps to mitigate cyber threats, and ensure everyone can participate in the digital economy as it develops while combating online harassment. The pillars of the Digital Declaration are intended to ensure the internet is kept as an open platform for expression and a driver of innovation." (Verizon, 2019, p. 47).

These statements, taken together, indicate a high-justice NMPv orientation.

The Warrior NMPv Orientation (High Justice-Low Control):

Warrior organisations in the NMPv Orientation Matrix are not driven by compliance alone and often associate privacy with ethics and trust. Similar to the Citizenship NMPv orientation, the Warrior NMPv orientation expresses privacy as an organisational value, rather than a compliance requirement. Organisations in the Warrior *(n=5)* and Citizenship (*n=2)* NMPv orientation reported evidence of NMPv activities driven by stakeholder trust. Apple was the only organisation in the Warrior NMPv orientation who did not report this activity. In the Warrior NMPv orientation, Allstate, a financial institution, was the only organisation who did not report on collaborations with advocacy groups.

The Warrior NMPv orientation includes the NMPv activities of the Citizenship NMPv orientation, however they may also exhibit less control than the Citizenship NMPv orientation. For example, they may choose non-compliance if they feel that compliance would breach an individual's privacy rights. It is noteworthy that in 2017, three organisations in the Warrior orientation (Apple, Cisco and Microsoft) together with both organisations in the Citizenship orientation (AT&T and Verizon) filed amicus briefs appealing the U.S. law enforcement decision to force Microsoft to hand over data about an Irish customer (Microsoft, 2020). Six organisations are positioned in the Warrior NMPv orientation, and interestingly all except Allstate are categorised as technology firms (Allstate, Apple, Cisco, IBM, HP, Microsoft). Cisco is presented as an exemplar of the Warrior NMPv orientation below.

The Warrior NMPv Orientation Exemplar:

Cisco is classified by the Fortune index in the Technology industry. Its technologies include infrastructure platforms; applications; security and other products. Infrastructure Platforms consists of its core networking technologies of switching, routing, data centre products and wireless that are designed to work together to deliver networking capabilities and transport and store data[8]. Cisco offers software and hardware for networking and data centres, and security products that include threat management products, threat security products. Thus, Cisco sells products and services that can be used to provide privacy/security assurance, and therefore the protection of data is of foremost importance to their business and reputation. The Cisco materiality assessment, as outlined in Figure 5.7, shows that 'data security and privacy' is important to both the business and its stakeholders, and is framed as a 'society' issue.

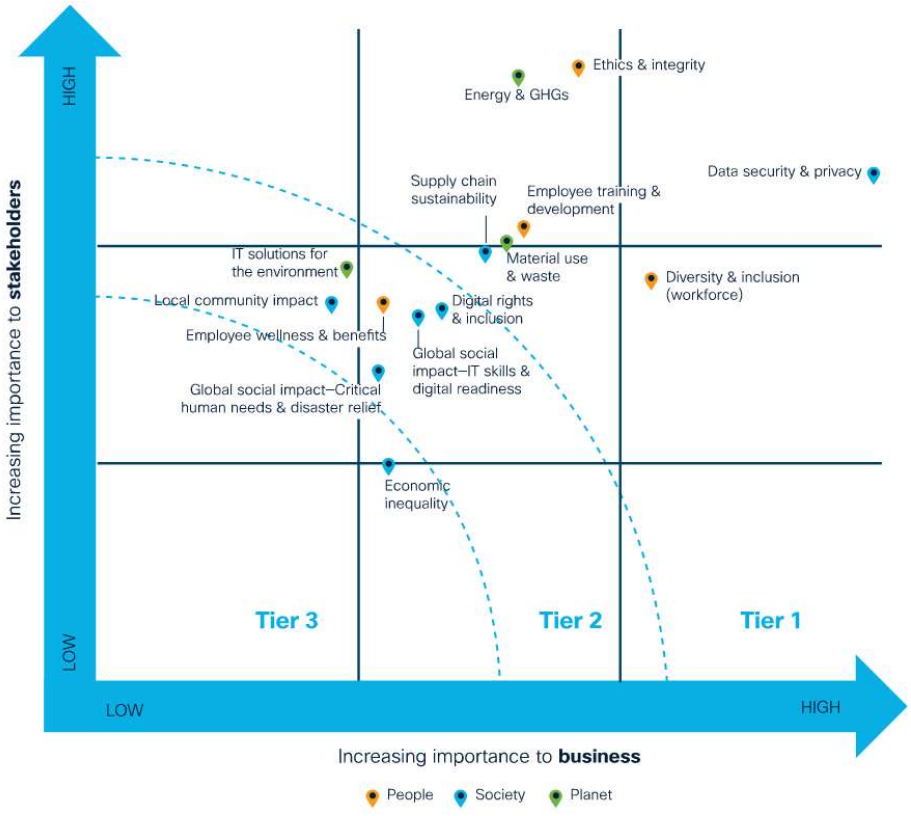


Figure 5.6 Cisco's Materiality Assessment (Cisco, 2019, p. 28)

[8] https://www.reuters.com/companies/CSCO.OQ

Similar to the Citizenship NMPv orientations, many of the organisations in the Warrior NMPv orientation will exceed regulation, for instance by producing reports and studies, and entering into collaborations that are aimed at improving privacy for society. Collaborating with other organisations regarding privacy is a high-justice NMPv activity with a weighting of 5 in the Nonmarket Privacy Activities Codebook. Cisco reported the production of an annual Data Privacy Benchmark Study aimed at highlighting the business value of good data privacy, which is made available to the public. Cisco report more privacy related collaborations than any other organisation in the sample. Figure 5.8 lists the collaborations reported by Cisco. The extent of the collaborations provides evidence of a high justice orientation.

Actions	Collaborations	
Participating in groups including:	· Internet Engineering Task Force · Internet Governance Forum · Institute of Electrical and Electronic Engineers (IEEE) Standards Association · International Standards Organization (ISO) · National Institute of Standards and Technology (NIST) · International Telecommunications Union · World Wide Web Consortium	· Cloud Security Alliance · Health Information Trust Alliance · National Cyber Security Alliance (NCSA) · Payment Card Industry (PCI) Board of Advisors · Centre for Information Policy Leadership (CIPL) · Future of Privacy Forum · Center for Democracy and Technology · International Association of Privacy Professionals (IAPP)
Supporting data privacy certifications such as:	· EU/Swiss-US · EU Binding Corporate Rules	· APEC Cross Border Privacy Rules · APEC Privacy Recognition for Processors
Influencing global privacy law and regulatory guidance in:	· APEC Member Economies · ASEAN · European Union · United States · Canada	· Brazil · China · Singapore · Japan · Vietnam
Leading development of privacy standards like:	· IEEE · ISO · EU Cloud Code of Conduct	

Figure 5.7 Cisco's Reported Collaborations (Cisco, 2019, p. 111)

Organisations with a Warrior NMPv orientation focus on strengthening privacy for society, and thus evidence of political perspectives of NMPv are often present in reports. For example, Cisco report:

"We're committed to respecting privacy as a human right, helping to shape new regulations and industry standards to protect privacy while supporting data-driven innovation, and working with our customers, partners, peers, and others to do the same….in FY19…we recommended that the U.S. develop an omnibus federal privacy law ensuring a consistent baseline of protection…..Cisco is leading the development of privacy frameworks around the world. We're speaking out in support of policies that favor interoperable global standards and a safe, free, and open Internet capabilities that enhance network security can be deployed by end users to subvert these principles. (Cisco, 2019, p.111)

Organisations in this orientation will also position privacy as a strategic priority, and advocate for greater data privacy and protection. For example, in the Cisco report, their CEO Chuck Robbins is quoted:

"We see massive opportunities for our innovation, expertise, and culture to play a role in finding solutions to some of society's biggest challenges…including partnering with governments to accelerate digitization goals and advocating for data security and privacy." (Cisco, 2019, p.3)

Organisations in the Warrior NMPv orientation, provide evidence that they perceive privacy as not just a data protection issue but a societal issue also – and thus often frame privacy as a human right:

"In FY19, Cisco called for comprehensive U.S. federal data protection legislation anchored to core principles of transparency, fairness, and accountability, because privacy is a human right". (Cisco, 2019, p.111).

Cisco dedicate an entire section of their CSR report – to privacy as a human right. Cisco have also supplemented their human rights policy with six human rights position statements that describe Cisco's approach to key emerging human rights challenges in the technology sector, These challenges include encryption, privacy and government surveillance. Most notable for the Warrior NMPv orientation, Cisco have also dedicated an entire section of their CSR report to what it refers to as its 'Position on Government Use of Technology to Curtail Freedom of Expression'. Cisco provide systems that enable encryption, and also provide systems that allow deep-state packet inspection in order to provide for operability. Their systems can be misused for state surveillance and privacy

invasion. Cisco abdicates responsibility for any misuse of their systems by nation states, and hence cannot exercise complete 'control' over their systems. Cisco explicitly comment in their CSR report how despite their commitment to protecting privacy, their systems can be used to compromise privacy:

> *"Unfortunately, there is no effective way to provide network administrators the capabilities necessary to protect their networks (and end-users) without also putting at their disposal powerful security capabilities which can be exploited in ways that can impair free expression. Disabling these security technologies would put networks, and the users of those networks, at risk. ….While leading DPI technologies have been designed to protect the security of network end-users, press reports for more than a decade have alleged their (mis)use by governments to facilitate the control and censorship of the flow of information, blocking access to unfavored websites, and restricting the use of encrypted communication tools."(Cisco, 2019, p. 211).*

5.3 Chapter Conclusion

The Nonmarket Privacy Orientation Matrix is a novel, theoretically derived framework – underpinned by theories of CSR and theories of control and justice. The results of the thematic analysis of the CSR reports, and the positions of the organisations on the Nonmarket Privacy Orientation Matrix, help to validate the theorised NMPv activities within each of the orientations of the Nonmarket Privacy Orientation Matrix. Greenaway et al. (2015) call for the construction of a mechanism that can measure and position an organisation's privacy orientation, distinguished by 'the extent to which control and justice provisions are manifested in privacy policies (Greenaway et al., 2015). Responding to this call, this chapter described the process of positioning an organisation's NMPv orientation, distinguished "by the extent to which control and justice provisions are manifested in their 'CSR reports' rather than their 'privacy policies'. The chapter also demonstrated the utility of the Nonmarket Privacy Activities Codebook, by applying it to the CSR reports of the organisations listed in the Fortune 100 index, and positioning them in one of the four orientations of the Nonmarket Privacy Orientation Matrix.

6 CHAPTER SIX: STUDY TWO – QUANTITATIVE ANALYSIS

6.1 Introduction

This chapter presents the results of the empirical work undertaken for Study Two. As discussed in Chapter 4, Study Two involves two experiments. The first experiment is concerned with empirically exploring the relationship between levels of control and justice signalled by Corporate Political Privacy activities i.e. privacy lobbying, with privacy concern, consumer trust, and purchase intention. The second experiment builds on the results of the first, by exploring the influence that levels of control and justice have on the relationship between both types of NMPv activities i.e., Corporate Political Privacy and Corporate Social Privacy, with privacy concern, consumer trust, and continuance intention. The chapter begins by presenting a visual overview of the two experiments, as outlined in Figure 6.1.

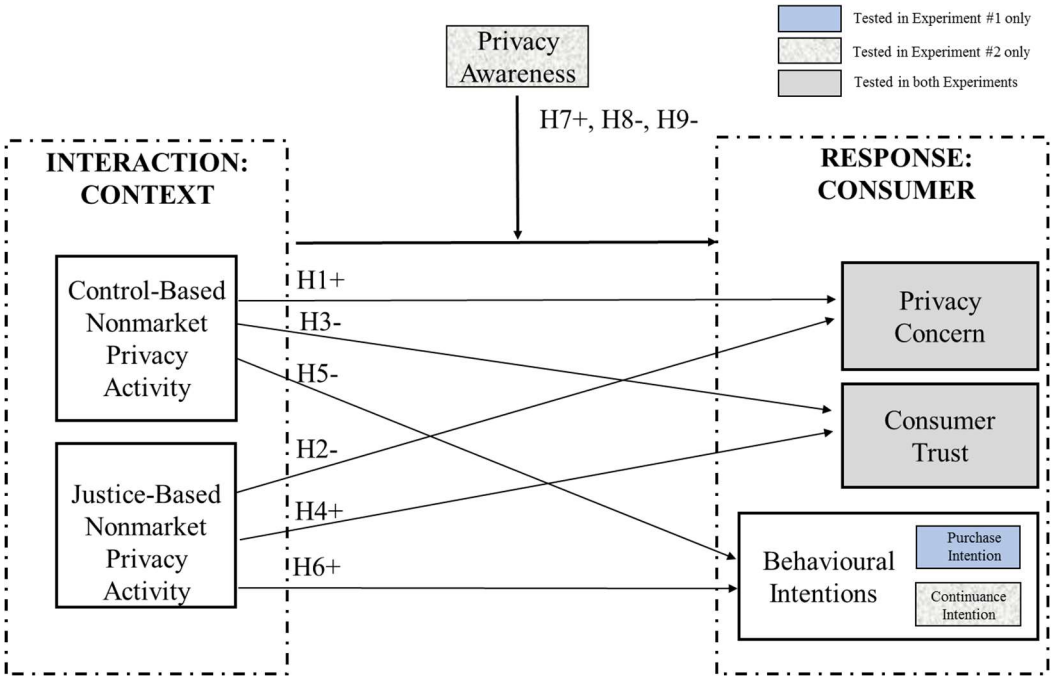


Figure 6.1 Overview of the Two Experiments in Study Two

Analysis of each experiment is presented separately, and organised into four key steps, namely; (i) data screening, (ii) descriptive statistics, (iii) analysis of variance (ANOVA) tests with random respondent effect, and finally (iv) support for hypotheses. The chapter concludes with a summary of results for the hypotheses in each experiment.

6.2 Experiment 1

The particular NMPv activity selected for Experiment 1, was a Corporate Political Privacy activity, more specifically, privacy lobbying. The proposed research model for Experiment 1 is presented in Figure 6.2.

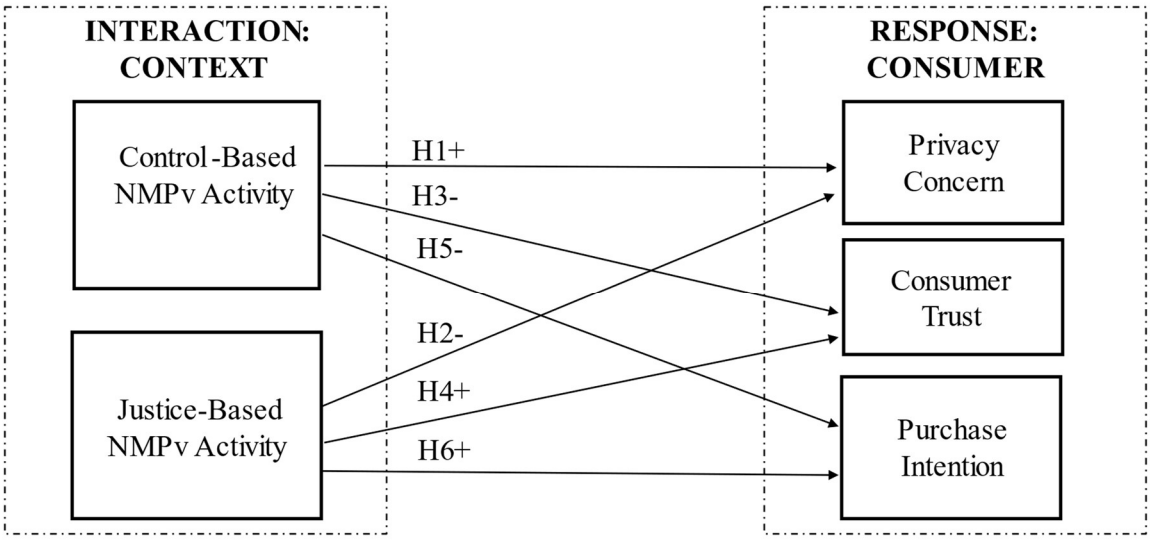


Figure 6.2 Experiment 1 Proposed Research Model

6.2.1 Data Screening and Validity.

Data screening and cleaning was performed in order to fulfil the requirements for performing multivariate analysis. Accordingly, an assessment of missing data, outliers, multicollinearity and normality were carried out.

6.2.1.1 Incomplete or Inaccurate Data

Raw data were screened, and responses eliminated, on the basis of three tests. First, two attention check questions (ACQs) were used to screen out inattentive respondents, as advised by Aust et al. (2013), and Buhrmester et al. (2011). Second, in order to assess the participants' understanding of the manipulations, a manipulation check question was also included, as advised by Hauser et al. (2018). Third, a standard bot-detection check question in Qualtrics 'I am not a robot', was used to ensure responses were not automated. An incorrect response to any of these three questions, resulted in the survey failing. If the participant successfully completed the survey, a random 4-digit completion code was generated by Qualtrics and had to be input by the participant into AMT. The sample started with 958 survey records. Incomplete surveys, and those with failed ACQs accounted for 330 failed survey records and these were deleted. 628 records remained. Of the remaining 628 records, 232 records failed the manipulation check question (Hauser et al., 2018) and these records were also removed. The final data set consisted of 396 successfully completed surveys.

6.2.1.2 Correlations, Multicollinearity and Normality

Bivariate correlation analysis was conducted using Pearson's correlation coefficient for two reasons. First, to examine the relationships among the demographic variables, the dependent variables, the control variables, and the experimental conditions. The experimental condition (the manipulation of beneficiary) is referred to as 'ManBnf', and there are four separate experimental conditions; Vignette 1, Vignette 2, Vignette 3 and Vignette 4. Second, to determine if multicollinearity problems existed. A correlation value of 0.7 or higher is generally considered an indicator of multicollinearity (Yu et al., 2015). On examining the correlation matrix, as outlined in Table 6.2, such concerns do not exist.

Table 6.1 Experiment 1 Pearson's Correlations

Variables	*M*	*SD*	α	1	2	3	4	5	6	7	8	9	10
1 ManBnf	-	-	-	1									
2 Privacy concern	3.78	1.11	.964	-.514**	1								
3 Consumer trust	2.679	1.312	.941	.616**	-.650**	1							
4 Purchase intention	2.74	1.26	.927	.592**	-.647**	.862**	1						
5 Propensity to trust	3.408	1.07	.891	.005	.035	.128*	.107*	1					
6 Disposition to privacy	3.641	.886	.807	-.007	.217**	.008	-.034	.055	1				
7 Age	-	-	-	-.106*	-.118*	-181**	-.141**	.080	-.057	1			
8 Nationality	-	-	-	-.019	.027	.001	.000	.054	.048	-.077	1		
9 Gender	-	-	-	.012	.092	-.049	-.060	-.030	-.060	.065	-.094	1	
10 Occupation	-	-	-	-.063	.031	-.074	-.055	-.070	-.073	.136**	.042	-.020	1

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

The correlation matrix indicates that propensity to trust is significantly, and positively, correlated with consumer trust *(r*=.13, *p*=.05), and disposition to value privacy is significantly, and positively, correlated with privacy concern (*r*=.22, *p*=.01). Purchase intention is also significantly and positively correlated with consumer trust (*r*=.86, *p*=.01) and privacy concerns (*r*=-.65, *p*=.01). These correlations again were expected, as empirical studies have previously found support for these relationships. As expected, ManBnf is positively correlated with consumer trust (*r*=.62, *p*=.01), privacy concern (*r*= -.51, *p*=.01), and purchase intention (*r*=.59, *p*=.01). However ManBnf is also positively correlated with age (*r*=-.11, *p*=.05). Age was also found to have a significant correlation with the dependent variables - privacy concern (*r*=.12, *p*=.05), consumer trust (*r*=.18, *p*=.01) and purchase intention (*r*=-.14, *p*=.05). The choices resulting from these statistical results were to either use age to represent an alternative hypothesis (Spector and Brannick, 2011) or to use age as a control variable during testing for main effects, to determine if age had a predictive effect on any of the dependent variables. Given the specific objectives of the research, it was decided to use age as a control variable. However future research could explore the influence of age on the dependent variable further.

In order to test for normality, the distribution of each variable was visually explored using histograms, and the skewness and kurtosis of all items was also reviewed. None of the items breached the kurtosis threshold of +/- 2.2 required for demonstrating normal univariate distribution (George and Mallery, 2010). Table 6.3 presents the skewness results for all variables, which lie between -1 and 1 across the dataset, suggesting a relatively normal distribution.

6.2.1.3 Construct Means, Reliability and Validity across Conditions

Means, standard deviation for all continuous variables were calculated for each experimental condition and are presented in Table 6.2. The means across the experimental

groups were similar for the control variables and were varied for the dependent variables. The psychometric properties of the measures were tested using Cronbach's alpha (Cronbach, 1951) as a measure of reliability. Results for Cronbach's Alpha (α) are also presented in Table 6.2. For early stages of research, Nunnally (1967, 1978) suggested a cut-off of 0.7, and for basic research, Nunnally suggested a more stringent cut-off of 0.80 or higher (Lance et al., 2006). In business management research, one tends to see 0.8 cited as a minimum Cronbach alpha (Sekaran, 2003). Internal consistency for all constructs was acceptable as all coefficients are above the recommended values. In this way, the psychometric properties of the measures were deemed appropriate.

Table 6.2 Experiment 1 Comparison of Means, Standard Deviations, Reliability across Conditions

Variables	Vignette 1 *n=101* M (SD)	Vignette 2 *n=96* M (SD)	Vignette 3 *n=98* M (SD)	Vignette 4 n=101 M (SD)	(α)	Skewness	Kurtosis
Consumer trust *(4 items)*	1.80 (.994)	1.75 (1.000)	3.53 (.918)	3.61 (.928)	.964	.059	-1.394
Privacy concern *(4 items)*	4.40 (.642)	4.36 (.799)	3.34 (1.08)	3.04 (1.145)	.941	-.752	-.427
Purchase intention *(3 items)*	1.96 (.998)	1.87 (.994)	3.48 (.948)	3.63 (.876)	.927	.001	-1.311
Propensity to trust *(4 items)*	3.27 (1.09)	3.58 (1.039)	3.47 (1.058)	3.32 (1.096)	.891	-.627	-.468
Disposition to privacy *(3 items)*	3.71 (.876)	3.58 (.904)	3.57 (.883)	3.70 (.887)	.807	-.495	-.074

6.2.2 Main Effects Analysis and Hypotheses Support

This section first presents the tests conducted for ANOVA assumptions, the results of the ANOVA, the ANCOVA and then the regression analysis, and then outlines support for the hypotheses.

6.2.2.1 ANOVA Assumptions Testing

ANOVA has several assumptions that must be met prior to interpretation (Leech et al., 2015). The first is that the data is normally distributed, which can be determined by analysing skewness (Leech et al., 2015). As previously noted, skewness indicates a relatively normal distribution (see Table 6.2). The second is that all observations are independent. ANOVA assumes that the observations are random and that the samples taken from the populations are independent of each other. Independence of observations can only be achieved if an experiment is set up correctly. There is no way to use the study's data to test whether independence has been achieved; rather, independence is achieved by correctly randomising sample selection (Scariano and Davenport, 1987). The distribution of vignettes across the sample demographic demonstrates the success of randomisation across the data set. The third is that the variances of each group are approximately equal i.e., homogeneity of variance. The Levene's statistic was calculated for the dependent and control variables, and results are outlined in Table 6.3. As a rule of thumb, population variances are not equal if $p<.05$ (Whittier et al., 2019). Levene's test showed that the variances for consumer trust (L=.35, p=.786) were equal and variances for purchase intention (L=.42, p=.749) were equal. Privacy concern (L=18, p=.001) does not meet the assumption. However, ANOVA is generally considered robust to violations of this assumption when sample sizes across groups are equal, as is the case in this experiment (Kim and Cribbie, 2017). So even with a significant result for Levene's test, moderately different variances are not a problem in balanced datasets, so long as the largest variance is more than 9 times the smallest variance (Keppel, 1991). Thus, the homogeneity of variance assumptions for ANOVA are still adequate.

Table 6.3 Experiment 1 Tests Of Homogeneity Of Variances

	Levene Statistic	df1	df2	Sig.
Privacy concern	18.032	3	392	.001
Consumer trust	.354	3	392	.786
Purchase intention	.420	3	392	.739
Propensity to trust	.701	3	392	.552
Disposition to value privacy	.276	3	392	.843
Age	1.849	3	392	.138
Nationality	2.087	3	392	.101
Gender	1.832	3	392	.141

6.2.2.2 Group Equivalence Across Variables

Once the assumptions for ANOVA were successfully tested, a series of one-way ANOVAs were conducted to assess for the presence of between-group differences for the dependent, demographic and control variables across the four experimental conditions. Table 6.4. presents the results of the ANOVA.

Table 6.4 Experiment 1 One Way ANOVA for All Variables across the Conditions

	Sum of Squares	Df1/Df2	Mean Square	F	Sig.
Privacy concern	145.670	3/392	48.557	54.978	.001
Consumer trust	318.889	3/392	106.296	115.143	.001
Purchase intention	269.656	3/392	89.885	98.558	.001
Propensity to trust	5.845	3/392	1.948	1.691	.168
Disposition to value privacy	1.750	3/392	.583	.740	.529
Age	30.190	3/392	10.063	1.859	.136
Nationality	.554	3/392	.185	.527	.664
Gender	.266	3/392	.089	.375	.771

As expected, the control variables (propensity to trust and disposition to value privacy), were found to be stable variables that did not change from one manipulation condition to the next. The results suggest that the random assignment of participants to the four experimental conditions was effective in approximating group equivalence on the control variables associated with the dependent variables, as per Price et al. (2015). As expected, there was a statistically significant variation in all three dependent variables across the vignettes, demonstrating that the manipulations were successful i.e., consumer trust: (F(3, 392)=115.14; p<.001), privacy concern: (F(3,392)=54.98; p<.001), and purchase intention: (F(3,392)=98.56; p<.001)).

Whilst several studies have empirically analyzed the relationships between privacy concern and demographic characteristics such as income level, level of education, and gender (Hoofnagle et al., 2010; O'Neil, 2001; Paine et al., 2007; Sheehan and Hoy, 2000; Taddicken, 2014; Youn, 2009), there is no consensus as to whether gender affects privacy concern (Lee et al., 2019). Studies which recognise the significance of the relationship between gender and privacy concern have taken a consistent viewpoint that women feel higher privacy concern than men. For example, Omarzu (2000) found that gender affects the evaluation of online privacy concern and Sheehan and Hoy (2000) found that female respondents were relatively more concerned about privacy infringement when asked to provide personal information by online marketers. Similarly, according to Graeff and Harmon (2002), females have higher privacy concern than males. Other studies have indicated that gender is not a significant factor in relation to privacy concern (Jensen et al., 2005; Zhang et al., 2013; Zukowski and Brown, 2007). Jensen et al. (2005) found no statistically significant differences by gender in the level of privacy concern. To adjust for any effect caused by the control variables, an ANCOVA was conducted for each dependent variable. Table 6.5 presents the ANCOVA results. The ANCOVA tells us the significance of the relationship between the independent variable (ManBnf) and the dependent variable,

but not the strength. Therefore, estimates for effects size (ή2) were calculated and are also presented together with the ANCOVA results.

Table 6.5 Experiment 1 ANCOVA Results for the Dependent Variables

	Type III Sum of Squares	df	Mean Square	F	Sig.	ή2
Privacy concern	139.816	3	46.605	56.695	.001	.304
Privacy concern adj [a]	171.292	5	34.258	41.675	.001	.348
[a] *Covariates appearing in the model are: disposition to value privacy and age*						
Consumer trust	305.752	3	101.917	117.330	.001	.474
Consumer trust adj [b]	342.000	5	68.400	78.744	.001	.502
[b] *Covariates appearing in the model are: propensity to trust and age*						
Purchase intention	260.252	3	86.751	95.711	.001	.423
Purchase intention adj [c]	272.764	4	68.191	75.234	.001	.435
[c] *Covariates appearing in the model are: age*						

There were some small changes in the adjusted means for the dependent variables. Disposition to value privacy and age accounted for an additional 4% (ή2 change = .04) of the variance in privacy concern scores. Propensity to trust and age accounted for an additional 3% (ή2 change = .03) of the variance of consumer trust scores. Age accounted for an additional 1% (ή2 change = .01) of the variance in purchase intention. These results indicate that the control variables have little predictive effect on the dependent variables across the vignettes.

6.2.2.3 Hypotheses Testing

Neither the ANCOVA nor ANOVA tell us the differences between vignette groups, only if group variances are significant. To determine the nature of group differences, multiple pairwise comparison (post-hoc) analysis using Tukey's honest significance difference (HSD) test was conducted (See Table 6.6).

Table 6.6 Experiment 1 Multiple Comparisons (Post-Hoc Tukey HSD)

DV	(I) Vignette	(J) Vignette	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval Lower Bound	95% Confidence Interval Upper Bound
Privacy Concern	1 (HighC)	2 (HigherC)	.046	.133	.985	-.298	.392
		3 (HighJ)	1.069*	.133	.001	.725	1.413
		4 (HigherJ)	1.3613*	.132	.001	1.022	1.702
	2 (HigherC)	3 (HighJ)	1.022*	.134	.001	.674	1.370
		4 (HigherJ)	1.3146*	.133	.001	.969	1.660
	3 (HighJ)	4 (HigherJ)	.292	.133	.127	-.051	.635
Consumer Trust	1 (HighC)	2 (HigherC)	.044	.136	.988	-.309	.397
		3 (HighJ)	-1.733*	.136	.001	-2.085	-1.382
		4 (HigherJ)	-1.809*	.135	.001	-2.158	-1.460
	2 (HigherC)	3 (HighJ)	-1.777*	.137	.001	-2.133	-1.422
		4 (HigherJ)	-1.853*	.136	.001	-2.207	-1.500
	3 (HighJ)	4 (HigherJ)	-.075	.136	.945	-.427	.275
Purchase Intention	1 (HighC)	2 (HigherC)	.089	.136	.914	-.262	.440
		3 (HighJ)	-1.525*	.135	.001	-1.875	-1.176
		4 (HigherJ)	-1.676*	.134	.001	-2.023	-1.329
	2 (HigherC)	3 (HighJ)	-1.614*	.137	.001	-1.968	-1.261
		4 (HigherJ)	-1.765*	.136	.001	-2.116	-1.414
	3 (HighJ)	4 (HigherJ)	-.150	.135	.682	-.500	.198

*. *The mean difference is significant at the 0.05 level.*

The Tukey HSD test revealed that variance between high-justice conditions i.e. Vignette 3 and Vignette 4, and high-control conditions i.e. Vignette 1 and Vignette 2, was significant across all three dependent variables. The variance between both justice conditions i.e. Vignette 3 and Vignette 4, was small across all three dependent variables, and was not statistically significant (p>.05). The variance between both control conditions i.e. Vignette 1 and Vignette 2, was also small across all three variables, and again not statistically significant (p>.05). In the remainder of this section, these results are presented and discussed in the following order: privacy concern, consumer trust and purchase intention.

Privacy Concern

For ANCOVA results, see relevant extract from Table 6.6, below:

	Type III Sum of Squares	df	Mean[2]	F	Sig.	ή2
Privacy concern	139.816	3	46.605	56.695	.001	.304
Privacy concern adj [a]	171.292	5	34.258	41.675	.001	.348

[a] *Covariates appearing in the model are disposition to value privacy and age*

Using guidelines for effect size from Cohen (1998), the strength of the relationship between privacy concern and the varying levels of ManBnf (whilst controlling for disposition to value privacy and age) is strong (ή2=.35).

H1 states that Corporate Political Privacy activities expressing high levels of control will lead to increased levels of privacy concern when compared to Corporate Political Privacy activities expressing high levels of justice. It was hypothesised in H2 that Corporate Political Privacy activities expressing high levels of justice will lead to decreased levels of privacy concern compared to Corporate Political Privacy activities expressing high levels of control. Based on the results of the ANCOVA Tukey test results, as outlined in Table 6.7, support for hypotheses H1 and H2 is indicated by the following:

First, privacy concern mean scores were statistically significantly lower in the high-justice condition Vignette 3 (*M*=3.30, *SD*= 1.08, *p*<.001) and the higher-justice condition Vignette 4 (*M*=3.04, *SD*=1.10, *p*<.001) when compared with the high-control condition Vignette 1 (*M*=4.4, *SD*=.64, *p*<.001) and the higher-control condition Vignette 2 (*M*=4.35, *SD*=.80, *p*<.001). Privacy concern mean scores increase by 1.36 between high control and higher justice conditions. Second, mean scores for privacy concern in the high-control conditions of Vignette 1 (*M*=4.40, *SD*=.64) and Vignette 2 (*M*=4.30, *SD*=.79), are statistically significantly greater than the mean scores for privacy concern in the high-justice conditions of Vignette 3 (*M*=3.34, *SD*=1.08) and Vignette 4 (*M*=3.04, *SD*=1.14). This suggests high-control Corporate Political Privacy activities lead to increased privacy concern compared

to high-justice Corporate Political Privacy activities. Also noted in the Tukey HSD results is a small increase in mean scores for privacy concern between the high-control condition of Vignette 1 and the higher-control condition of Vignette 2, that was not statistically significant (p=.985). This suggests that as control levels increase from high to higher, privacy concern also increases slightly (mean difference = .04). Also noted is a slight decrease in mean scores for privacy concern between the high-justice condition of Vignette 3 and the higher-justice condition of Vignette 4, that was not statistically significant (p=.127). This suggests that as justice levels increase from high to higher, privacy concern also decreases slightly (mean difference= -.29). Thus, support for H1 and H2 is indicated. These variations are plotted in Figure 6.3, to help visualise the effects of the vignette conditions on mean scores for privacy concern.

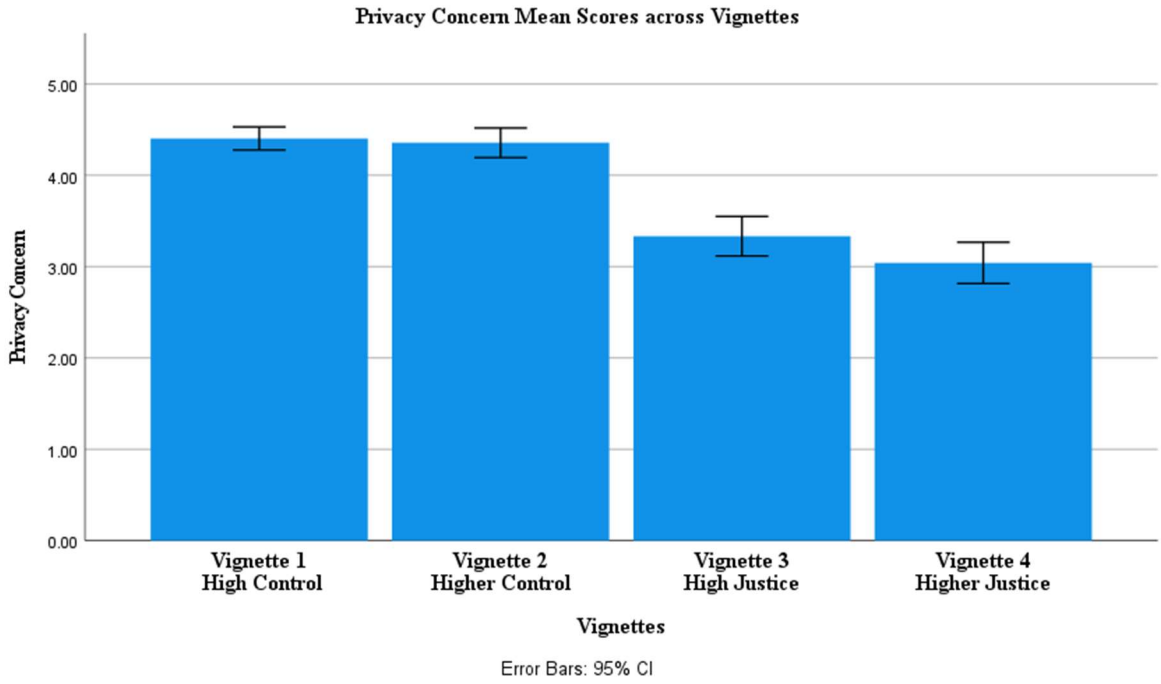


Figure 6.3 Experiment 1 Privacy Concern Mean Scores across Vignettes

Consumer Trust

For ANCOVA results, see relevant extract from Table 6.6. below:

	Type III Sum of Squares	df	Mean[2]	F	Sig.	ή2
Consumer trust	305.752	3	101.917	117.330	.001	.474
Consumer trust adj [b]	342.000	5	68.400	78.744	.001	.502

[b] *Covariates appearing in the model are: propensity to trust and age*

Using guidelines for effect size from Cohen (1998), the strength of the relationship between consumer trust and the varying levels of ManBnf (whilst controlling for propensity to trust and age) is strong (ή2=.50).

H3 states that Corporate Political Privacy activities expressing high levels of control were expected to lead to decreased levels of consumer trust compared to Corporate Political Privacy activities expressing g high levels of justice. H4 states that Corporate Political Privacy activities expressing high levels of justice were expected to lead to increased levels of consumer trust compared to Corporate Political Privacy activities expressing high levels of control. Based on the results of the ANCOVA Tukey tests, as outlined in Table 6.7, support for hypotheses H3 and H4 is indicated by the following:

First, in the Tukey HSD results, mean scores for consumer trust in the control conditions of Vignette 1 (*M*=1.79, *SD*=.99) and Vignette 2 (*M*=1.75, *SD*=.10) are significantly less than the mean scores for consumer trust in the justice conditions of Vignette 3 (*M*=3.53, *SD*=.92) and Vignette 4 (*M*=3.6, *SD*=.92). This indicates that control-based Corporate Political Privacy activities lead to less consumer trust than justice-based Corporate Political Privacy activities. Also noted in the Tukey HSD results is a statistically not significant (*p*=.988) but slight decrease in mean scores for consumer trust between the high-control condition of Vignette 1 and the higher-control condition of Vignette 2. This indicates that as control levels increase from high to higher, consumer trust also decreases slightly (mean difference=.04). Also noted is a small but not significant *(p*=.945) increase in mean scores

for consumer trust between the high-justice condition of Vignette 3 and the higher-justice condition of Vignette 4. This indicates that as justice levels increase from high to higher, consumer trust also increases slightly (mean difference = .07). These variations are plotted in Figure 6.4, to visualise the effects of the vignette conditions on mean scores for consumer trust. Second, also evident in the Tukey HSD results is that consumer trust mean scores were statistically significantly higher in the high-justice condition Vignette 3 (M=3.53, SD=.92, p<.001) and the higher-justice condition Vignette 4 (M=3.60, SD=.93, p<.001) when compared with the high-control condition Vignette 1 (M=1.80, SD=.99, p<.001) and the higher-control condition Vignette 2 (M=1.75, SD=1, p<.001).

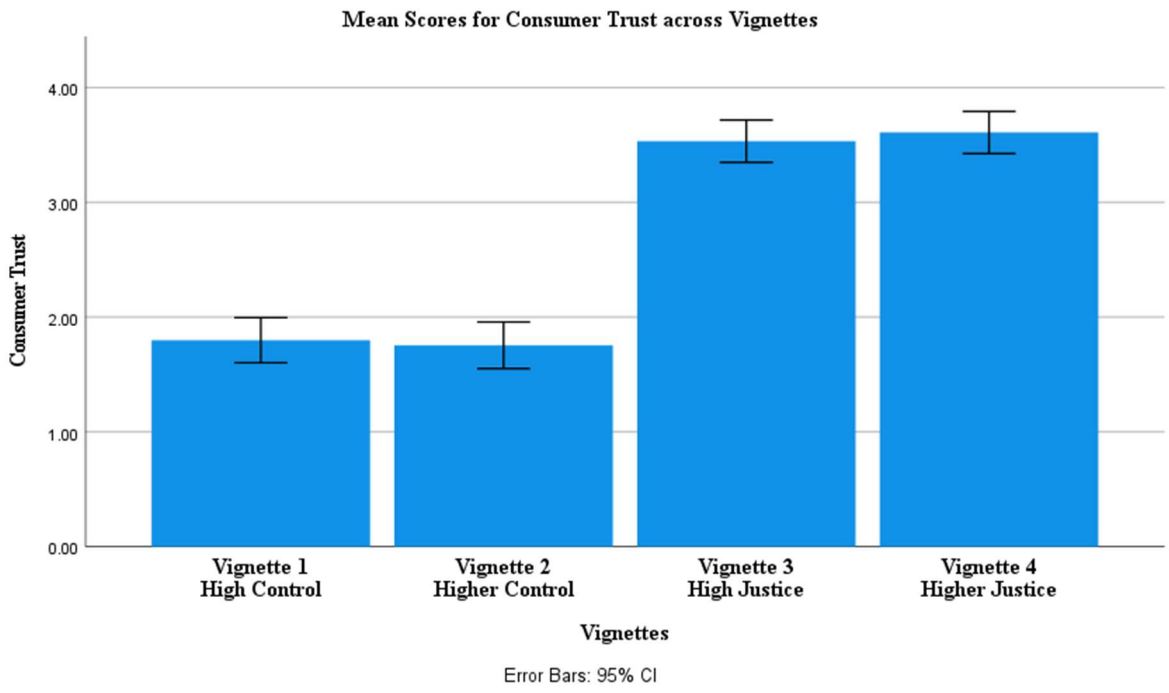


Figure 6.4 Experiment 1 Consumer Trust Mean Scores across Vignettes

Purchase Intention

For purchase intention ANCOVA results, see relevant extract from Table 6.6 below:

	Type III Sum of Squares	df	Mean[2]	F	Sig.	ή2
Purchase intention	260.252	3	86.751	95.711	.001	.423
Purchase intention adj [c]	272.764	4	68.191	75.234	.001	.435

[c] *Covariates appearing in the model are age*

Using guidelines for effect size from Cohen (1998), the strength of the relationship between purchase intention and the varying levels of ManBnf (whilst controlling for age) is strong (ή2=.435).

H5 states that Corporate Political Privacy activities expressing high levels of control were expected to lead to decreased levels of purchase intention compared to Corporate Political Privacy activities expressing high levels of justice. Corporate Political Privacy states that Corporate Political Privacy activities expressing high levels of justice were expected to lead to increased levels of purchase intention compared to CPPv activities expressing high levels of control. Based on the results of the ANCOVA Tukey tests, as outlined in Table 6.7, support for hypotheses H5 and H6 is indicated by the following:

Firstly, mean scores were statistically significantly higher in the high-justice condition Vignette 3 (3.48 =/- .94, p<.001) and the higher-justice condition Vignette 4 (M=3.63, SD=.87, p<.001) when compared with the high-control condition Vignette 1 (M=1.95, SD= 1, p<.001) and the higher-control condition Vignette 2 (M=1.86, SD=1, p<.001). Secondly, mean scores for purchase intention in the control conditions of Vignette 1 *(*M=1.95, SD=.99) and Vignette 2 (M=1.87, SD=.99) are significantly less than the mean scores for purchase intention in the justice conditions of Vignette 3 (M=3.48, SD=.94) and Vignette 4 (M=3.63, SD=.87). This indicates lower purchase intention for high-control Corporate Political Privacy activities and higher purchase intention for high-justice Corporate Political Privacy activities. Also noted in the Tukey tests results is a small

decrease in mean scores for purchase intention between the high-control condition of Vignette 1 and the higher-control condition of Vignette 2 (mean difference =-.09) that is not statistically significant (p=.914). Also noted is a small increase in mean scores for purchase intention between the high-justice condition of Vignette 3 and the higher-justice condition of Vignette 4 (mean differences=+.15), that was not statistically significant (p=.682). This would indicate that varying the level of justice signalled by Corporate Political Privacy from 'high' to 'higher' or varying the level of control from 'high' to 'higher' influences purchase intention. Thus, support for H5 and H6 is indicated. These variations are plotted in Figure 6.5, to visualise the effects of the vignette conditions on mean scores for purchase intention.

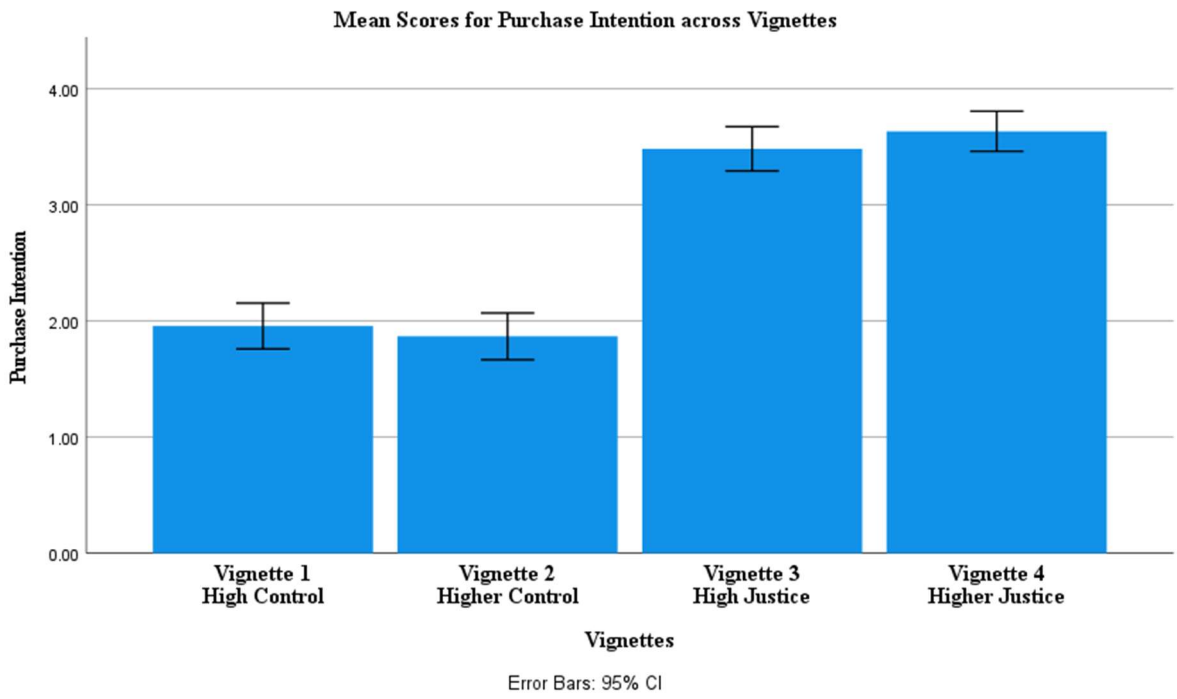


Figure 6.5 Experiment 1 Purchase Intention Mean Scores across Vignettes

6.3 Experiment 2

The first experiment found support for all hypotheses. However, the vignettes tested levels of control and justice only for Corporate Political Privacy activities. The second experiment was designed to build on this, by including both of the NMPv strategies i.e. Corporate Social Privacy and Corporate Political Privacy, along with investigating the role of important moderating factors i.e., privacy awareness. Similar to the first experiment, the second experiment consists of four vignettes, as outlined in Section 4.6.2.3. In each vignette, the NMPv activity is described as either a Corporate Political Privacy activity or as a Corporate Social Privacy. The research model for Experiment 2 is outlined in Figure 6.6. This model outlines the hypotheses, the key relationships, the dependent variables and the moderator variables. In the remainder of this section, data screening and validity, analysis for main effects and support for the hypotheses are discussed.

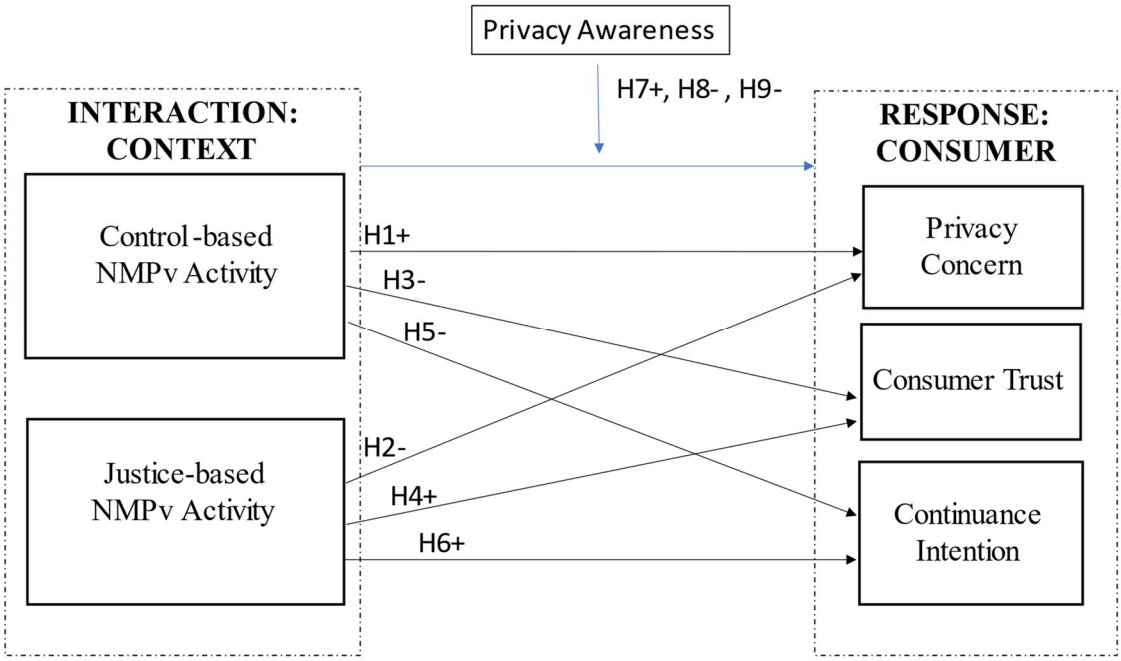


Figure 6.6 Experiment 2 Proposed Research Model

6.3.1 Data Screening and Validity

Data screening and cleaning was performed in order to fulfil the requirements for performing multivariate analysis. Accordingly, an assessment of missing data, outliers, multicollinearity and normality were carried out.

6.3.1.1 Incomplete or Inaccurate Data

The three tests conducted in Experiment 1 were repeated for Experiment 2, i.e., ACQs, manipulation checks and BOT detection checks. There were 948 survey records. After removing surveys with no completion codes, i.e. those that failed the ACQs, or the manipulation check, or the BOT detection check, a final set (n=508) of completed surveys was compiled.

6.3.1.2 Correlations, Multicollinearity and Normality

Multicollinearity generally occurs when there are high correlations between two or more predictor variables (Vogt, 2005). In other words, one predictor variable can be used to predict the other. This creates redundant information, skewing the results in a regression model. An easy way to detect multicollinearity is to calculate correlation coefficients for all pairs of predictor variables. Correlation coefficients were conducted using Pearson's correlation in order to examine the relationships among the variables and the experiment condition, and to test if multicollinearity problems existed. If the correlation coefficient value is 0.7 or higher, this is generally considered an indicator of multicollinearity. See Table 6.7, for the results of Pearson's correlation, showing that multicollinearity concerns did not exist.

Table 6.7 Experiment 2 Pearson's Correlation Matrix

	M	SD	α	1	2	3	4	5	6	7	8	9	10	11	12
1. ManBnf	-	-	-	1											
2. Privacy concern	3.5425	1.0466	.948	-.154**	1										
3. Consumer trust	3.5837	1.19402	.868	.232**	-.506**	1									
4. Continuance intention	3.5368	1.23222	.937	.170**	.820**	-.519**	1								
5. Propensity to trust	3.5094	1.0078	.875	.019	.306**	-.138**	.308**	1							
6. Disposition to privacy	3.7473	.8632	.852	.007	.021	.351**	-.058	-.037	1						
7. Perceived need government surveillance	2.4439	1.3343	.955	-.060	.280**	.175**	.315**	.306**	.159**	1					
8. Political affiliation (social)	3.5807	1.8298	-	.065	.142**	.176**	.149**	.159**	.230**	.364**	1				
9. Political affiliation (economic)	3.9665	1.7566	-	.005	.054	.199**	.048	.133**	.209**	.247**	.736**	1			
10. Privacy awareness	3.6929	.8565	-	.026	.202**	.064	.215**	.229**	.292**	.149**	.082	.082	1		
11. Age	-	-	-	.079	-.062	.058	-.035	.044	-.015	-.208**	.030	.072	.049	1	
12.Gender	-	-	-	.004	.074	-.070	.111*	.110*	-.003	-.002	.096*	.134**	-.006	.072	1

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

As expected, ManBnf is significantly correlated with consumer trust (r=.23, p=.01), privacy concern (r=-.15, p=.01) and continuance intention (r=.17, p=.01). Propensity to trust was expected to be correlated with consumer trust (r=.31, p=.01) however propensity to trust was also found to be significantly correlated with privacy concern (r=-.14, p=.01) and continuance intention (r=.31, p=.01)). Interestingly, privacy awareness is not significantly correlated with privacy concern (r=.02, p=.05), but is significantly correlated with consumer trust (r=.20, p=.01) and continuance intention (r=.21, p=.001). There are several other correlations between the control variables and the dependent variables that are statistically significant. The additional control variables; perceived need for government surveillance, political affiliation (social), political affiliation (economic), are significantly correlated with the dependent variables. Perceived need for government surveillance is significantly correlated with consumer trust (r=.28, p=.01), privacy concern (r=.17, p=.001) and continuance intention (r=.31, p=.01). Political affiliation (social) is also significantly correlated with consumer trust *(*r=.14, p=.01), privacy concern (r=.17, p=.01) and continuance intention (r=.14, p=.01). Political affiliation (economic) is only significantly correlated with privacy concern (r=.2, p=.01). For the demographic variables, gender is significantly correlated with continuance intention (r=.11, p=.05) only. Age is not significantly correlated with any of the dependent variables but is significantly correlated with perceived need for government surveillance *(*r=-.21, p=.05). Variables that have a significant correlation with the dependent variables, are included as covariates when testing for main effects.

6.3.1.3 Construct Means, Reliability, Validity Across Conditions

Means and standard deviation were calculated for each experimental condition and are presented in Table 6.8. The means across the experimental groups were similar for the control variables and were varied for the dependent variables. The psychometric properties of the measures were tested using Cronbach's alpha (Cronbach, 1951), with results for

Cronbach's Alpha (α) presented in Table 6.8. Internal consistency for all constructs was acceptable i.e., 0.8 (Sekaran, 2003). In this way, the psychometric properties of the measures were deemed appropriate.

Table 6.8 Experiment 2 Comparison of Means, Standard Deviations, Reliability Across Conditions

Variables	Vignette 1 *n=130* M (SD)	Vignette 2 *n=132* M (SD)	Vignette 3 *n=122* M (SD)	Vignette 4 n=134 M (SD)	(F)	(P)	Cronbach (α)	Skewness	Kurtosis
Privacy Concern *(10 items)*	4.40 (.642)	2.94 (1.1)	3.92 (.794)	3.26 (1.03)	50.31	.001	.948	-.788	-.193
Consumer Trust *(4 items)*	2.86 (1.32)	4.2 (.704)	3.18 (1.25)	4.03 (.764)	55.55	.001	.868	-.839	-.345
Continuance Intention *(3 items)*	2.87 (1.361)	4.2 (.75)	3.24 (.123)	3.81 (1.04)	45.37	.001	.937	-.707	-.603
Propensity to Trust *(4 items)*	3.45 (1.03)	3.54 (1.02)	3.54 (.938)	3.5 (1.03)	.235	.872	.875	-.979	.007
Disposition to Privacy *(3 items)*	3.74 (.864)	3.7 (.867)	3.8 (.823)	3.73 (.902)	.318	.813	.852	-.638	-.001
Perceived need For Gov Surveillance *(4 items)*	2.55 (1.33)	2.28 (1.27)	2.78 (1.32)	2.15 (1.32)	5.68	.001	.955	.347	-1.376
Political Affiliation (Social) *(1 item)*	3.53 (1.87)	3.36 (1.85)	3.65 (1.67)	3.79 (1.9)	1.264	.286		.110	-1.155
Political Affiliation (Economic) *(1 item)*	3.99 (1.84)	3.86 (1.69)	4.06 (1.66)	3.95 (1.82)	.291	.832	-	-.142	-1.002
Privacy Awareness *(4 items)*	3.67 (.927)	3.64 (.83)	3.79 (.771)	3.67 (.888)	.781	.505	.801	-.648	-.242

6.3.2 Main Effects Analysis and Hypotheses Support

This section first presents the tests conducted for the assumptions of ANOVA and its results, and then presents the results of ANCOVA and Regression analyses. The section concludes with an overview of support for the hypotheses.

6.3.2.1 ANOVA Assumptions Testing

Tests for ANOVA assumptions were conducted prior to interpretation. The first test is that all observations are independent. This assumption is met by AMT and the sampling selection. The second test is homogeneity of variance; that is, that the variances of each group are approximately equal. Levene's test showed that the variances for all the dependent variables were not equal, as outlined in Table 6.9, i.e., privacy concern (L=17.08, p=.001), consumer trust (L=57.25, p=.001), and continuance intention (L=34.57, p=.001). The dependent variables do not meet the assumption, however the ANOVA is generally considered robust to violations of this assumption when sample sizes across groups are equal, as is the case in Experiment 2. The final assumption is that the dependent variable is normally distributed, which can be determined by analysing its' skewness (Leech et al., 2015). The distribution of each variable was visually explored using histograms, and the skewness and kurtosis of all items are outlined in Table 6.8. None of the items breached the kurtosis threshold of +/- 2.2 required for proving normal univariate distribution (George and Mallery, 2010). Skewness for all variables lies between -1 and 1 across the dataset, which infers a relatively normal distribution.

Table 6.9 Experiment 2 Equality of Means/ Homogeneity of Variances (Levene's)

	Levene	df1	df2	Sig.
Privacy concern	17.089	3	504	.001
Consumer trust	57.256	3	504	.001
Continuance intention	34.573	3	504	.001
Propensity to trust	.672	3	504	.570
Disposition to value privacy	.502	3	504	.681
Perceived need for government surveillance	.724	3	504	.538
Political affiliation (social)	1.883	3	504	.131
Political affiliation (economic)	1.247	3	504	.292
Privacy awareness	1.907	3	504	.127

6.3.2.2 Group Equivalence Across Variables

Once these tests for assumptions were successful, a one-way ANOVA was conducted to assess for the presence of between-group differences in the dependent, control and moderator variables across the four experimental conditions. See Table 6.13 for the results of the ANOVAs across the groups. There was a statistically significant variation in mean scores for all three dependent variables across the vignettes, indicating that the manipulations were successful. consumer trust (F=50.31, p<.001), privacy concern (F=41.56, p<.001), continuance intention (F=36.09, p<.001). The results suggest that the random assignment of participants to the four experimental conditions was effective in approximating group equivalence on the control variables associated with the dependent variables. With the exception of perceived need for government surveillance (F=5.68, p<.001), there were no statistically significant variations in mean scores for the control variables. Perceived need for government surveillance was included as a control variable.

Table 6.10 Experiment 2 ANOVA Results Across Conditions

	Sum of Squares	df	Mean Square	F	Sig.
Privacy concern	110.163	3	36.721	41.569	.001
Consumer trust	166.590	3	55.530	50.316	.001
Continuance intention	136.131	3	45.377	36.091	.001
Propensity to trust	.719	3	.240	.235	.872
Disposition to value privacy	.713	3	.238	.318	.813
Perceived need for government surveillance	29.545	3	9.848	5.685	.001
Political affiliation (social)	12.679	3	4.226	1.264	.286
Political affiliation (economic)	2.708	3	.903	.291	.832
Privacy awareness	1.720	3	.573	.781	.505
Age	21.704	3	7.235	1.375	.250
Gender	1.303	3	.434	1.724	.161

To adjust for any variance potentially caused by the control variables, an ANCOVA was conducted for the dependent variables. Table 6.11 presents the ANCOVA results across the manipulated conditions. Whilst the ANCOVA tells us the significance of the relationship between the vignette condition and the dependent variable, accounting for the effect of covariates, it does not describe the strength of the relationship. Therefore estimates for effects size (ή2) were calculated and are also presented in Table 6.11.

Table 6.11 Experiment 2 ANCOVA Results, Adjusted for Covariates

	Type III Sum of Squares	Df	Mean Square	F	Sig.	ή2
Privacy concern						
Corrected Model[a]	194.150	8	24.269	33.524	.001	.350
Intercept	82.089	1	82.089	113.397	.001	.185
Propensity to trust	12.830	1	12.830	17.723	.001	.034
Disposition to value privacy	43.852	1	43.852	60.576	.001	.108
Perceived need for gov surveillance	3.145	1	3.145	4.344	.038	.009
Polit affiliation (social)	.014	1	.014	.020	.889	.000
Polit affiliation (economic)	3.438	1	3.438	4.750	.030	.009
ManBnf	93.355	3	31.118	42.986	.001	.205

[a] *Covariates appearing in the model are evaluated at these values: propensity to trust=3.5, disposition to privacy = 3.74, perceived need for government surveillance=2.44, political affiliation (social) = 3.58, political affiliation (econ) = 3.96.*

Consumer trust						
Corrected Model[b]	285.666	6	47.611	54.565	.001	.395
Intercept	142.082	1	142.082	162.833	.001	.245
Propensity to trust	26.845	1	26.845	30.766	.001	.058
Perceived need for gov surveillance	48.617	1	48.617	55.717	.001	.100
Political affiliation (social)	.034	1	.034	.039	.843	.000
ManBnf	189.684	3	63.228	72.462	.001	.303

[b] *Covariates appearing in the model are evaluated at the following values: propensity to trust = 3.5094; perceived need for government surveillance= 2.4439,; political affiliation (social) = 3.5807.*

Continuance intention						
Corrected Model[c]	275.579	7	39.368	39.828	.001	.358
Intercept	76.112	1	76.112	77.000	.001	.133
Propensity to trust	25.220	1	25.220	25.514	.001	.049
Perc need for gov surveillance	60.547	1	60.547	61.253	.001	.109
Political affiliation (social)	.012	1	.012	.012	.914	.000
Gender	2.650	1	2.650	2.681	.102	.005
ManBnf	155.235	3	51.745	52.348	.001	.239

[c] *Covariates appearing in the model are evaluated at the following values, propensity to trust = 3.5094; perceived need for government surveillance= 2.4439: political affiliation (social)= 3.5807.*

6.3.2.3 Hypotheses Testing

Although it is evident that differences across the vignettes are statistically significant, ANOVA/ANCOVA does not tell which vignettes are significantly different from each other. Multiple pairwise comparison analysis using Tukey's honestly significant difference (HSD) test is conducted to determine the nature of variation across the vignettes. Table 6.12 outlines a summary of the Tukey HSD test results.

Table 6.12 Experiment 2 Multiple Comparisons (Tukey HSD)

Dependent Variable	(I) Vignette	(J) Vignette	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
						Lower Bound	Upper Bound
Consumer Trust	*1 CSPv_HC*	*2 CSPv_HJ*	-1.36186*	.12981	.001	-1.6965	-1.0273
		3 CPPv_HC	-.31917	.13242	.076	-.6605	.0222
		4 CPPv_HJ	-1.17100*	.13187	.001	-1.5109	-.8311
	2 CSPv_HJ	*3 CPPv_HC*	1.04269*	.13194	.001	.7026	1.3828
		4 CPPv_HJ	.19086	.13138	.467	-.1478	.5295
	3 CPPv_HC	*4 CPPv_HJ*	-.85183*	.13396	.001	-1.1971	-.5065
Privacy Concern	*1 CSPv_HC*	*2 CSPv_HJ*	1.11990*	.11614	.001	.8205	1.4192
		3 CPPv_HC	.14013	.11847	.638	-.1653	.4455
		4 CPPv_HJ	.80259*	.11798	.001	.4985	1.1067
	2 CSPv_HJ	*3 CPPv_HC*	-.97977*	.11804	.001	-1.2840	-.6755
		4 CPPv_HJ	-.31730*	.11754	.036	-.6203	-.0143
	3 CPPv_HC	*4 CPPv_HJ*	.66247*	.11985	.001	.3535	.9714
Continuance Intention	*1 CSPv_HC*	*2 CSPv_HJ*	-1.33217*	.13855	.000	-1.6893	-.9750
		3 CPPv_HC	-.37128*	.14134	.044	-.7356	-.0070
		4 CPPv_HJ	-.93978*	.14075	.000	-1.3026	-.5770
	2 CSPv_HJ	*3 CPPv_HC*	.96088*	.14082	.000	.5979	1.3239
		4 CPPv_HJ	.39239*	.14023	.027	.0309	.7538
	3 CPPv_HC	*4 CPPv_HJ*	-.56849*	.14299	.000	-.9371	-.1999

**. The mean difference is significant at the 0.05 level.*

The Tukey HSD test revealed differences across all three dependent variables. The results are discussed in the remainder of this section.

Privacy Concern

Using guidelines for effect size from Cohen (1998), the strength of the relationship between privacy concern and the varying levels of ManBnf (whilst controlling for disposition to value privacy and age) is strong (ή2=.35). See excerpt below from Table 6.12.

	Type III Sum of Squares	Df	Mean Square	F	Sig.	ή2
Privacy concern						
Corrected Model[a]	194.150	8	24.269	33.524	.001	.350
Intercept	82.089	1	82.089	113.397	.001	.185
Propensity to trust	12.830	1	12.830	17.723	.001	.034
Disposition to privacy	43.852	1	43.852	60.576	.001	.108
Perceived need for government surveillance	3.145	1	3.145	4.344	.038	.009
Political affiliation (social)	.014	1	.014	.020	.889	.000
Political affiliation (economic)	3.438	1	3.438	4.750	.030	.009
ManBnf	93.355	3	31.118	42.986	.001	.205

[a] *Covariates appearing in the model are evaluated at these values: propensity to trust=3.5, disposition to value privacy = 3.74, perceived need for government surveillance=2.44, political affiliation (economic) = 3.96, political affiliation (social) = 3.58*

H1 states that NMPv activities expressing high levels of control will lead to more privacy concern than NMPv activities expressing high levels of justice. H2 states that NMPv activities expressing high levels of justice will lead to less privacy concern than NMPv activities expressing high levels of control. A one-way ANCOVA was conducted with the vignette entered as the predictor variable, privacy concern entered as the dependent variable, controlling for disposition to value privacy, propensity to trust, perceived need for government surveillance, political affiliation (economic) and political affiliation (social). Support for hypotheses H1 and H2 is indicated by the following:

Privacy concern mean scores were statistically significantly lower in the high-justice Corporate Social Privacy condition Vignette 2 (2.93 =/- 1.1, *p*=.001) than the high-control Corporate Social Privacy condition of Vignette 1 (4.04 +/- .64, *p*=.001). Similarly, privacy concern mean scores were statistically significantly higher in the high-control Corporate Political Privacy condition Vignette 3 (3.92 =/- .79, *p*=.001) than the high-justice Corporate Political Privacy condition Vignette 4 (3.26 +/- 1.03, *p*=.001). The highest mean scores for privacy concern were found in the high-control Corporate Social Privacy condition of Vignette 1. This indicates decreased privacy concern for high-justice NMPv activities, and increased privacy concern for high-control NMPv activities. Thus, support for H1 and H2 is indicated. The results for privacy concern are plotted in Figure 6.7.

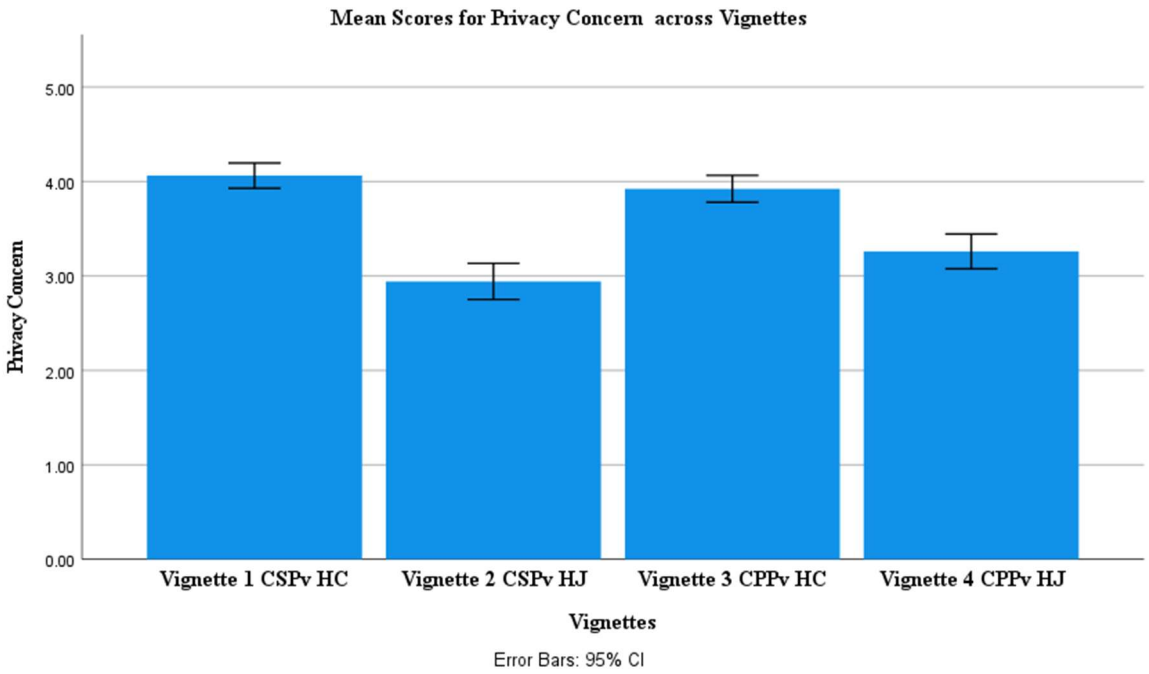


Figure 6.7 Experiment 2 Privacy Concern Mean Scores across Vignettes

Consumer Trust

The strength of the relationship between consumer trust and the varying levels of ManBnf (controlling for propensity to trust, disposition to value privacy, perceived need for government surveillance and political affiliation social) was also strong (ή2=.39). Perceived need for government surveillance accounted for 10% of the variance and propensity to trust an additional 5%. See excerpt below from Table 6.12.

	Type III Sum of Squares	Df	Mean Square	F	Sig.	ή2
Consumer Trust						
Corrected Model[b]	285.666	6	47.611	54.565	.001	.395
Intercept	142.082	1	142.082	162.833	.001	.245
Propensity to trust	26.845	1	26.845	30.766	.001	.058
Perceived need for government surveillance	48.617	1	48.617	55.717	.001	.100
Political affiliation (social)	.034	1	.034	.039	.843	.000
ManBnf	189.684	3	63.228	72.462	.001	.303

[b] *Covariates appearing in the model are evaluated at the following values: political affiliation (social)= 3.5807, perceived need for government surveillance = 2.4439, propensity to trust = 3.5094*

H3 states that NMPv activities expressing high levels of control will lead to less consumer trust than NMPv activities expressing high levels of justice. H4 states that NMPv activities expressing high levels of justice will lead to more consumer trust than NMPv activities expressing high levels of control. A one-way ANCOVA was conducted with ManBnf entered as the predictor variable, consumer trust as the dependent variable, controlling for disposition to value privacy, perceived need for government surveillance, and political affiliation (social). Based on the results of the ANCOVA, support for hypotheses H3 and H4 is indicated by the following:

Consumer trust mean scores were statistically significantly higher in the high-justice Corporate Social Privacy condition of Vignette 2 (*M*=4.22, *SD*=.70, *p*=.001) than the high-control Corporate Social Privacy condition of Vignette 1 (*M*=2.86, *SD*=1.32, *p*=.001).

Similarly consumer trust mean scores were statistically significantly higher in the high-justice Corporate Political Privacy condition of Vignette 4 (M=4.03, SD=.76, p=.001) than the high-control Corporate Political Privacy condition of Vignette 3 (M=3.18, SD=1.25, p=.001). The highest mean score for consumer trust was found in the high-justice Corporate Social Privacy condition of Vignette 2, and the lowest mean score for consumer trust was found in the high-control Corporate Social Privacy condition of Vignette 1.This indicates increased consumer trust for high-justice NMPv activities, and decreased consumer trust for high-control NMPv activities. Thus, support for H3 and H4 is indicated. The results for consumer trust are plotted in Figure 6.8.

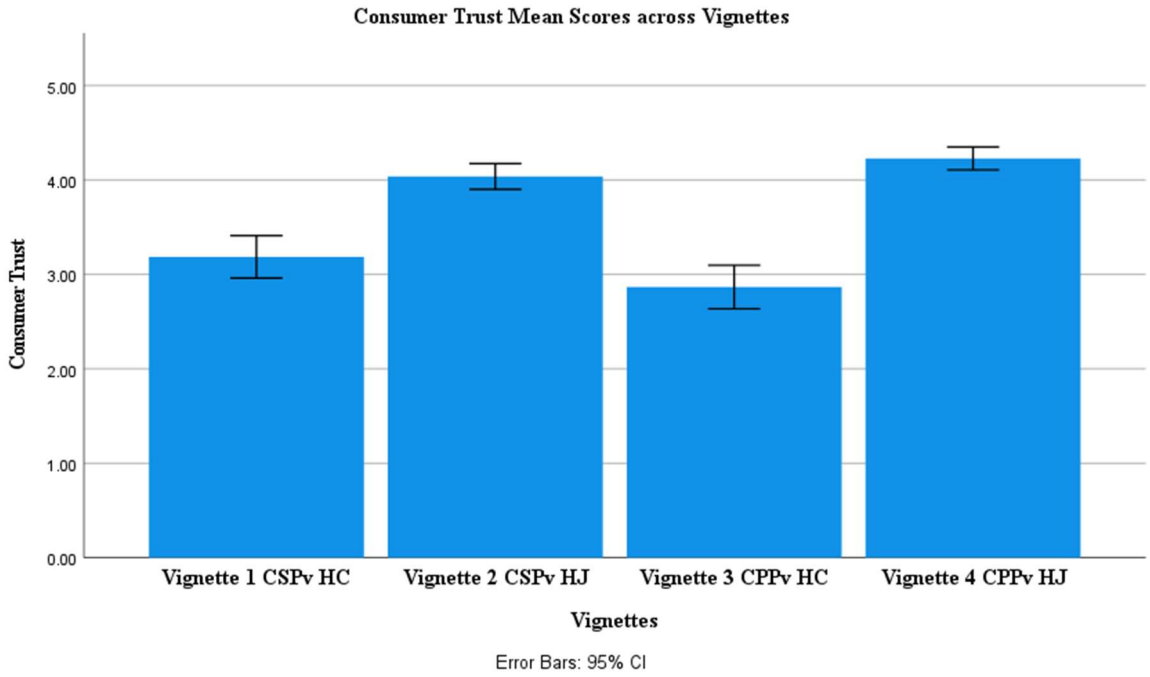


Figure 6.8 Experiment 2 Consumer Trust Mean Scores across Vignettes

Continuance Intention

The strength of the relationship between continuance intention (controlling for propensity to trust, perceived need for government surveillance, political affiliation social and gender) and the varying levels of ManBnf, was strong (ή2=.358). Again, perceived need for government surveillance accounted for 10% of the variance. See below excerpt from Table 6.12.

	Type III Sum of Squares	Df	Mean Square	F	Sig.	ή2
Continuance intention						
Corrected Model[c]	275.579	7	39.368	39.828	.001	.358
Intercept	76.112	1	76.112	77.000	.001	.133
Propensity to trust	25.220	1	25.220	25.514	.001	.049
Perceived need for government surveillance	60.547	1	60.547	61.253	.001	.109
Political affiliation (social)	.012	1	.012	.012	.914	.000
Gender	2.650	1	2.650	2.681	.102	.005
ManBnf	155.235	3	51.745	52.348	.001	.239

[c] *Covariates appearing in the model are evaluated at the following values: propensity to trust = 3.5094; political affiliation (social) = 3.5807, perceived need for government surveillance = 2.443.*

H5 states that NMPv activities expressing high levels of control will lead to less continuance intention than NMPv activities expressing high levels of justice. H6 states that NMPv activities expressing high levels of justice will lead to more continuance intention than NMPv activities expressing high levels of control. A one-way ANCOVA was conducted with ManBnf entered as the predictor variable, continuance intention entered as the dependent variable, controlling for propensity to trust, perceived need for government surveillance, political affiliation (social) and gender. Based on the results of the ANCOVA, support for hypotheses H5 and H6 is indicated by the following:

Continuance intention mean scores were statistically significantly higher in the high-justice Corporate Social Privacy condition of Vignette 2 (*M*=4.2, *SD*=.75, *p*=.001) than the high-control Corporate Social Privacy condition of Vignette 1 (*M*=2.87, *SD*=1.36, *p*=.001). Similarly continuance intention mean scores were statistically significantly higher in the

high-justice Corporate Political Privacy condition of Vignette 4 (M=3.81, SD= 1.04, p=.001) than the high-control Corporate Political Privacy condition of Vignette 3 (M=3.24, SD=1.2, p=.001). The highest mean scores for continuance intention were found in the high-justice Corporate Social Privacy condition of Vignette 2, and the lowest mean score for continuance intention was found in the high-control Corporate Social Privacy condition of Vignette 1.This indicates increased continuance intention for high-justice NMPv activities, and decreased continuance intention for high-control NMPv activities. Thus, support for H5 and H6 is indicated. The results for continuance intention are plotted in Figure 6.9.

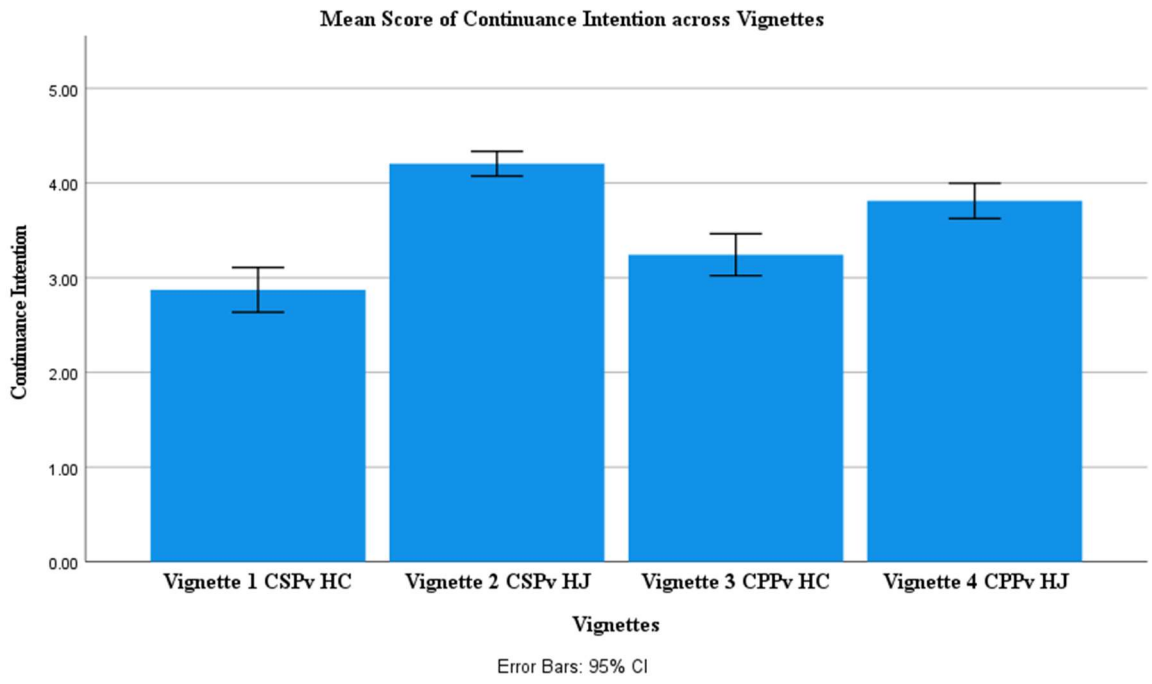


Figure 6.9 Experiment 2 Continuance Intention Mean Scores across Vignettes

6.3.2.4 Analysis For Moderation and Hypotheses Testing

H7 states that privacy awareness positively moderates the relationship between NMPv activities and privacy concern, such that the relationship is stronger when privacy awareness is high than when it is low. H8 states that privacy awareness negatively moderates the relationship between NMPv activities and consumer trust, such that the relationship is stronger when privacy awareness is low than when it is high. H9 states that

privacy awareness negatively moderates the relationship between NMPv activities and continuance intention, such that the relationship is stronger when privacy awareness is low than when it is high. The Two Way ANOVA/ANCOVA is frequently used to test for moderation, however West et al. (1996) highlight challenges with its use, when both independent variables are not continuous variables i.e., one is categorical, and one is continuous. Where the independent variable is a categorical variable and the moderator variable is a continuous variable, the use of a multiple regression approach is instead recommended (e.g., Baron and Kenny, 1986; Hayes and Rockwood, 2017, West et al., 1996). In this experiment, the independent variable is a categorical variable, and the moderator variable is a continuous variable. Thus, a moderated regression analysis, rather than a two way ANOVA, was conducted to test the effect of moderation.

First, an interaction variable called INTERACT was computed in SPSS, as the product of ManBnf and privacy awareness. There was a need to understand if the amount of variance accounted for *with the interaction* was significantly more than *without the interaction*. Regression analysis was then conducted. ManBnf and privacy awareness were the predictors in Model 1, and INTERACT as the additional predictor in Model 2. See Table 6.13 for results of the regression analysis. The results indicate that privacy awareness influences a significant change to the mean scores, from Model 1 without the interaction, to Model 2 with the interaction, for consumer trust and for continuance intention (at the .05 level) but not for privacy concern.

To further test for these effects, moderated regression analysis was again conducted using PROCESS (Hayes, 2018). PROCESS produces a number of models e.g.. mediation, moderated mediation and moderation etc. PROCESS Model 1 was selected, specifically the moderation model where the independent variable is a categorical variable, and both the moderator and dependent variable are a continuous variable. For each dependent variable, a regression was conducted: ManBnf was entered as the independent variable,

privacy awareness was entered as the moderating variable, and the dependent variables and control variables were changed for each regression.

Table 6.13 Experiment 2 Linear Regression (ANOVA and Model Fit)

Variable	Model	DF1/ DF2	Mean Square	F	Sig.	ΔR^2 (ΔF)	Sig* (ΔF)
Privacy Concern	Mode 1 Predictors: Privacy awareness, ManBnf	2/ 505	7.856	7.351	.000	.028 (7.35)	.001
	Model 2 Predictors: Privacy awareness, ManBnf, INTERACT	3/ 504	5.302	4.953	.002	.000 (.182)	.670
Consumer Trust	Model 1 Predictors: Privacy awareness, ManBnf	2/ 505	33.355	25.67	.000	.092 (25.67)	.001
	Model 2 Predictors: Privacy awareness, ManBnf, INTERACT	3/ 504	24.566	19.07	.000	.01 (5.42)	.020
Continuance Intention	Model 1 Predictors: Privacy awareness, ManBnf	2/ 505	28.184	19.949	.000	.073 (19.94)	.001
	Model 2 Predictors: Privacy awareness, ManBnf, INTERACT	3/ 504	21.850	15.637	.000	.012 (6.57)	.011

**. The difference is significant at the 0.05 level.*

PROCESS automatically constructs the interaction term (ManBnf x Privacy Awareness) required to test for moderation. To avoid potentially problematic high multicollinearity with the interaction term, PROCESS also standardises and centres the continuous variables (Aiken and West, 1991). The PROCESS output also tabulates a set of data (called regression matrix data) that can be plotted in order to visualise the interactions. The effects of ManBnf on the dependent variables, at -1SD, 0SD and +1SD of privacy awareness were

therefore plotted. This enables us to observe the slope of the regression lines visually using the 'pick-a-point' approach, to evaluate the moderating effect of privacy awareness at low, medium and high levels.

PROCESS Results

H7: To test the hypothesis that privacy awareness positively moderates the relationship between NMPv activities and privacy concern, see Table 6.13, which shows that ManBnf and privacy awareness accounted for a significant amount of variance in privacy concern: R^2 change =.03, p =.001. Model 1 without the interaction term is significant (F=7.35, p<.001). Model 2 with the interaction term is not significant (F=4.95, p>.001) and accounted for zero variance: R^2 change=0, p=.67 indicating that there is no significant moderating effect of privacy awareness on the relationship between ManBnf and privacy concern. A 'pick-a-point' visual analysis was conducted, using PROCESS (Hayes, 2018). See Figure 6.10 for the PROCESS interaction plots generated by the PROCESS regression analysis. The high justice-based lobbying activity (Vignette 4) was found to have a negative moderating effect on privacy concern, and no other effects were observed. H7 could therefore not be supported.

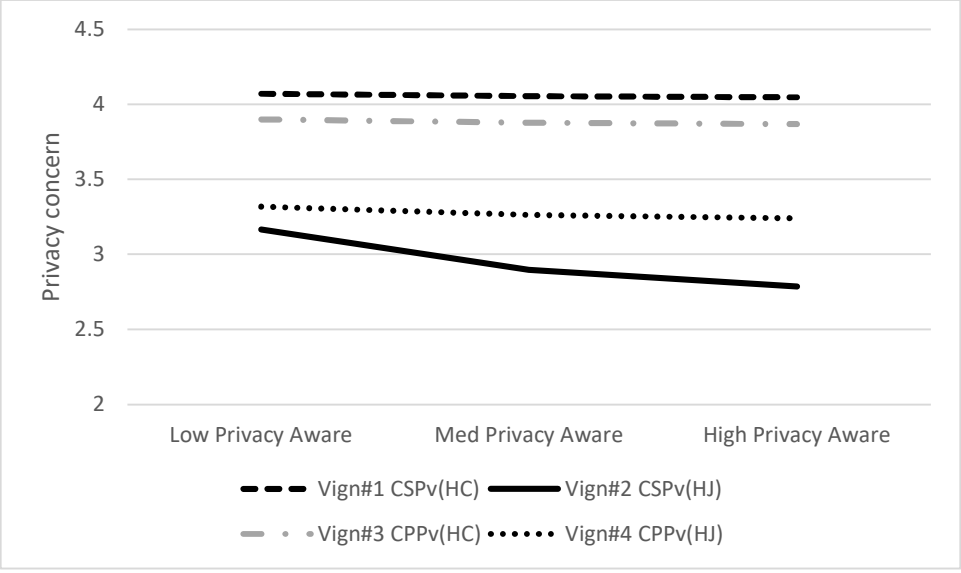


Figure 6.10 Experiment 2 Interaction Plot From PROCESS (Regression Analysis) Privacy Concern

H8: To test the hypothesis that privacy awareness negatively moderates the relationship between NMPv activity and consumer trust, see Table 6.13, which shows that ManBnf and privacy awareness accounted for a significant amount of variance in consumer trust: ΔR^2=.09, p< .001. Model 1 without the interaction term is significant (F=25.67, p<.001). Model 2 with the interaction term is also significant (F=19.07, p<.001), accounting for more variance than Model 1, although not significant: ΔR^2=.01,p=.02. This indicates that privacy awareness has a positive moderating effect on the relationship between ManBnf and consumer trust. See Figure 6.11, for the PROCESS interaction plots generated by the PROCESS regression analysis. For Vignette 1, Vignette 2 (control-based) and Vignette 3 (justice-based) – PROCESS records a positive moderating effect i.e., as privacy awareness rises, so too does consumer trust, and as privacy awareness decreases, consumer trust decreases. No moderating effect could be found for high justice-based lobbying activity (Vignette 4). Therefore H8 could not be supported.

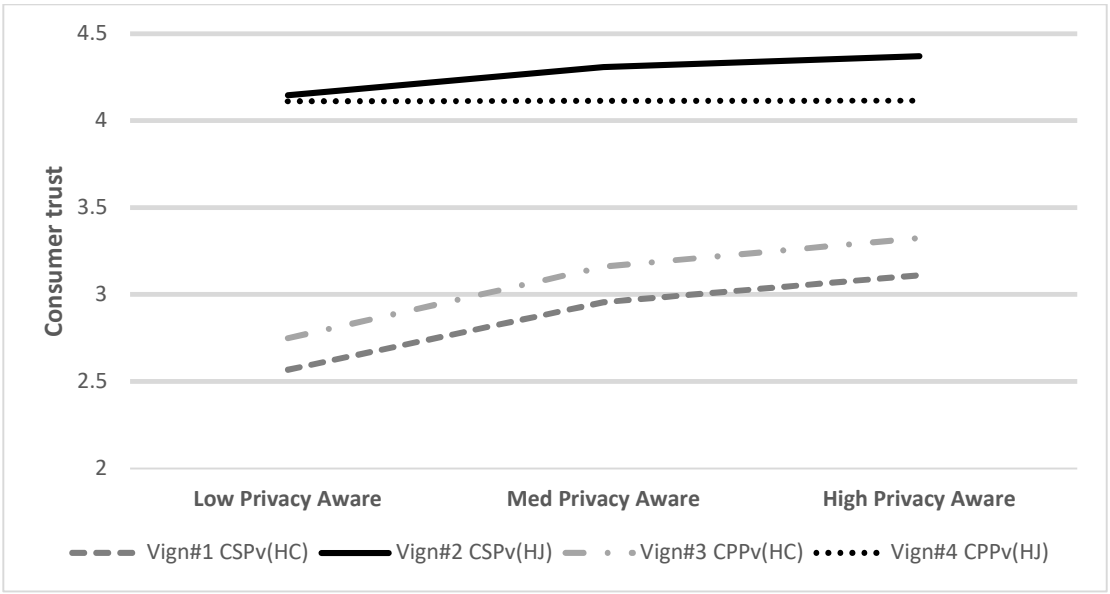


Figure 6.11 Experiment 2 Interaction Plot From PROCESS (Regression Analysis) Consumer Trust

H9: To test the hypothesis that privacy awareness negatively moderates the relationship between levels of control and justice signalled by an NMPv activity and continuance intention, see Table 6.16, which shows that Model 1 without the interaction term is significant (F=19.95, p<.001). Model 2, with the interaction term, is also significant (F=15.63, $p<.001$). Model 2, with the interaction between ManBnf and privacy awareness, accounted for more variance than Model 1, although not significant: R^2 change=.01, p=.01, indicating that privacy awareness has a positive moderating effect on the relationship between ManBnf and continuance intention. To examine the nature of the moderation effect in more detail a 'pick-a-point' visual analysis is conducted, again using PROCESS (Hayes, 2018). See Figure 6.12 for the PROCESS interaction plots generated by the PROCESS regression analysis. PROCESS records a small but positive moderating effect i.e., as privacy awareness rises, so too does continuance intention, and as privacy awareness decreases, so too does continuance intention - for both control-based and justice-based vignettes. Therefore H9 could not be supported.

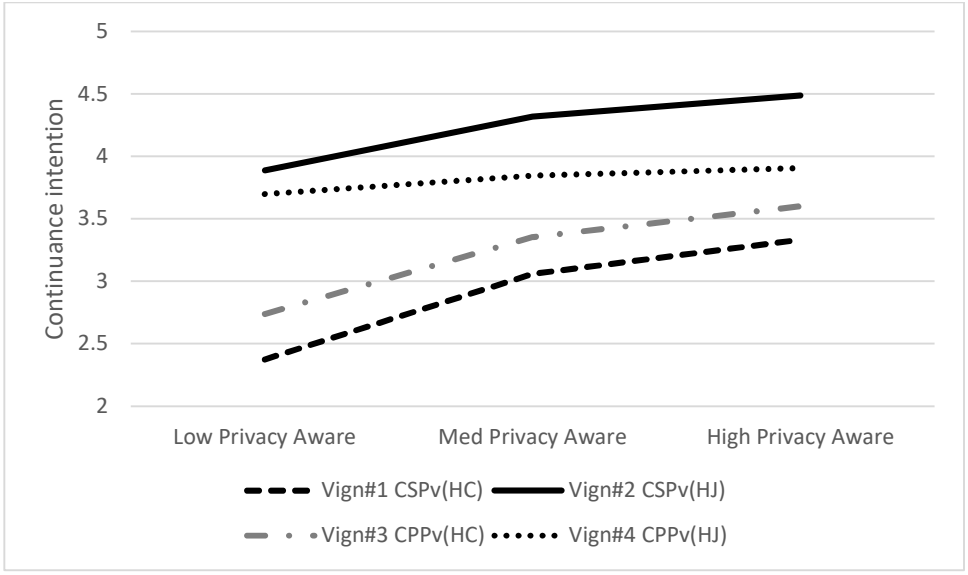


Figure 6.12 Experiment 2 Interaction Plot From PROCESS (Regression Analysis) Continuance Intention

6.4 Summary for Hypotheses Support in Both Experiments

Table 6.14 presents a summary of the hypotheses in Experiment 1.

Table 6.14 Experiment 1 Hypotheses Results Summary

Hypothesis	Finding	Variables	Support
H1: An organisation's reported NMPv activities signalling high levels of control are positively related to privacy concern	High-control Corporate Political Privacy activities positively influence privacy concern	ManBnf in Vignette 1 (CPPv-C). privacy concern	Fully Supported
	Higher-control Corporate Political Privacy positively influence privacy concern	ManBnf in Vignette 3 (CPPv-HC) privacy concern	Fully Supported
H2: An organisation's reported NMPv activities signalling high levels of justice are negatively related to privacy concern	High-justice Corporate Political Privacy activities negatively influence privacy concern	ManBnf in Vignette 2 (CPPv-J) privacy concern	Fully Supported
	Higher-justice Corporate Political Privacy activities negatively influence privacy concern	ManBnf in Vignette 4 (CPPv-HJ) privacy concern	Fully Supported
H3: An organisation's reported NMPv activities signalling high levels of control are negatively related to consumer trust	High-control Corporate Political Privacy activities negatively influence consumer trust	ManBnf in Vignette 1 (CPPv-C) consumer trust	Fully Supported
	Higher-control Corporate Political Privacy activities negatively influence consumer trust	ManBnf in Vignette 3 (CPPv-HC) consumer trust	Fully Supported
H4: An organisation's reported NMPv activities signalling high levels of justice are positively related to consumer trust	High-justice Corporate Political Privacy activities positively influence consumer trust	ManBnf in Vignette 2 (CPPv-J) consumer trust	Fully Supported
	Higher-justice Corporate Political Privacy activities positively influences consumer trust	ManBnf in Vignette 4 (CPPv HJ) consumer trust	Fully Supported
H5: An organisation's reported NMPv activities signalling high levels of control are negatively related to purchase intention	High-control Corporate Political Privacy activities negatively influences purchase intention	ManBnf in Vignette 1 (CPPv-C) purchase intention	Fully Supported
	Higher-control Corporate Political Privacy activities negatively influences purchase intention	ManBnf in Vignette 3 (CPPv-HC) purchase intention	Fully Supported
H6: An organisation's reported NMPv activities signalling high levels of justice are positively related to purchase intention	High-justice Corporate Political Privacy activities positively influences purchase intention	ManBnf in Vignette 2 (CPPv-J) purchase intention	Fully Supported
	Higher-justice Corporate Political Privacy activities positively influences purchase intention	ManBnf in Vignette 4 (CPPv-HJ) purchase intention	Fully Supported

NMPv = Nonmarket Privacy, C= Control, HC= Higher Control, J= Justice, HJ = Higher Justice, CPPv = Corporate Political Privacy

Table 6.15.presents a summary of the hypotheses in Experiment 2.

Table 6.15 Experiment 2 Hypotheses Results Summary

Hypothesis	Findings	Variables	Support
H1: An organisation's reported nonmarket privacy activities signalling high levels of control are positively related to privacy concern	Control-based Corporate Social Privacy activities positively influences privacy concern.	ManBnf in Vignette 1 (CSPv-HC) Privacy concern	Fully Supported
	Control-based Corporate Political Privacy activities positively influences privacy concern.	ManBnf in Vignette 3 (CPPv-HC) Privacy concern	Fully Supported
H2: An organisation's reported nonmarket privacy activities signalling high levels of justice are negatively related to privacy concern.	Justice-based Corporate Social Privacy activities negatively influences privacy concern.	ManBnf in Vignette 2 (CSPv-HJ) Privacy concern	Fully Supported
	Justice-based Corporate Political Privacy activities negatively influences privacy concern.	ManBnf in Vignette 4 (CPPv-HJ) Privacy concern	Fully Supported
H3: An organisation's reported nonmarket privacy activities signalling high levels of control are negatively related to consumer trust.	Control-based Corporate Social Privacy activities negatively influences consumer trust.	ManBnf in Vignette 1 (CSPv-HC) Consumer trust	Fully Supported
	Control-based Corporate Political Privacy negatively influences consumer trust.	ManBnf in Vignette 3 (CPPv-HC) Consumer trust	Fully Supported
H4: An organisation's reported nonmarket privacy activities signalling high levels of justice are positively related to consumer trust.	Justice-based Corporate Social Privacy activities positively influences consumer trust.	ManBnf in Vignette 2 (CSPv-HJ) Consumer trust	Fully Supported
	Justice-based Corporate Political Privacy activities positively influences consumer trust.	ManBnf in Vignette 4 (CPPv-HJ) Consumer trust	Fully Supported
H5: An organisation's reported nonmarket privacy activities signalling high levels of control are negatively related to purchase intention.	Control-based Corporate Social Privacy activities negatively influences continuance intention.	ManBnf in Vignette 1 (CSPv-HC), Continuance intention	Fully Supported
	Control-based Corporate Political Privacy activities negatively influences continuance intention.	ManBnf in Vignette 3 (CPPv-HC), Continuance intention	Fully Supported
H6: An organisation's reported nonmarket privacy activities signalling high levels of justice are positively related to purchase intention.	Justice-based Corporate Social Privacy activities positively influences continuance intention.	ManBnf in Vignette 2 (CSPv-HJ), Continuance intention	Fully Supported
	Justice-based Corporate Political Privacy activities positively influences continuance intention.	ManBnf in Vignette 4 (CPPv-HJ), Continuance intention	Fully Supported
H7: Privacy awareness positively moderates the relationship between nonmarket privacy activities and privacy concern, such that this relationship is stronger when privacy awareness is high than when it is low.	No significant moderation effects, however, privacy awareness negatively moderates the relationship between justice-based Corporate Political Privacy activities and privacy concern.	ManBnf, Privacy awareness, Privacy concern	Not Supported
H8: Privacy awareness negatively moderates the relationship between nonmarket privacy activities and consumer trust such that this relationship is stronger when privacy awareness is low than when it is high.	Privacy awareness positively moderates the relationship between nonmarket privacy activities and consumer trust.	ManBnf, Privacy awareness, Consumer trust	Not Supported
H9: Privacy awareness negatively moderates the relationship between nonmarket privacy activities and continuance intention, such that this relationship is stronger when privacy awareness is low than when it is high.	Privacy awareness positively moderates the relationship between nonmarket privacy activities and continuance intention.	ManBnf, Privacy awareness, Continuance intention	Not Supported

HC= High Control, HJ = High Justice, CPPv = Corporate Political Privacy, CSPv = Corporate Social Privacy

6.5 Chapter Conclusion

This chapter presented the quantitative analysis, procedures and findings. The chapter began with an overview of the experiments. Then, for each experiment, the data cleaning processes, the sample characteristics, the analysis for main effects were presented, followed in each case by a discussion of support for the hypotheses. Overall, the results from both experiments indicate that levels of control and justice signalled by NMPv activities influence privacy concern, consumer trust and purchase intention/continuance intention. The next chapter integrates and discusses the results of both the quantitative and qualitative phases of this research.

7 CHAPTER SEVEN: DISCUSSION AND CONCLUSIONS

7.1 Introduction

Whilst NMPV activities are increasingly being conducted by organisations, it remains an under-researched phenomenon. By filling this gap, this research presents a significant contribution not only to researchers but also to organisations – as they may be undertaking privacy activities that negatively impact their stakeholders, or may be missing opportunities to engage with privacy activities that positively impact both their stakeholders. To the best of the researcher's knowledge, this is the first time that NMPv has been investigated in this way.

The research follows a three-stage mixed-methods research design, to develop a more complete picture of NMPv activities, NMPv approaches, and how NMPv might influence the consumer. The overarching aim of this research is to establish a more comprehensive understanding of Nonmarket Privacy. This aim is represented by three key research questions, which are visually outlined in Figure 7.1, along with how these questions are addressed in this study.

This chapter revisits the three research questions, and discusses how the quantitative and qualitative findings respond to them. The findings and their implications are then considered in relation to these objectives. The unique contributions of the research are then discussed. This is followed by outlining the implications of this research for practice and policymakers. The chapter concludes by presenting the limitations of the research, along with avenues for future research.

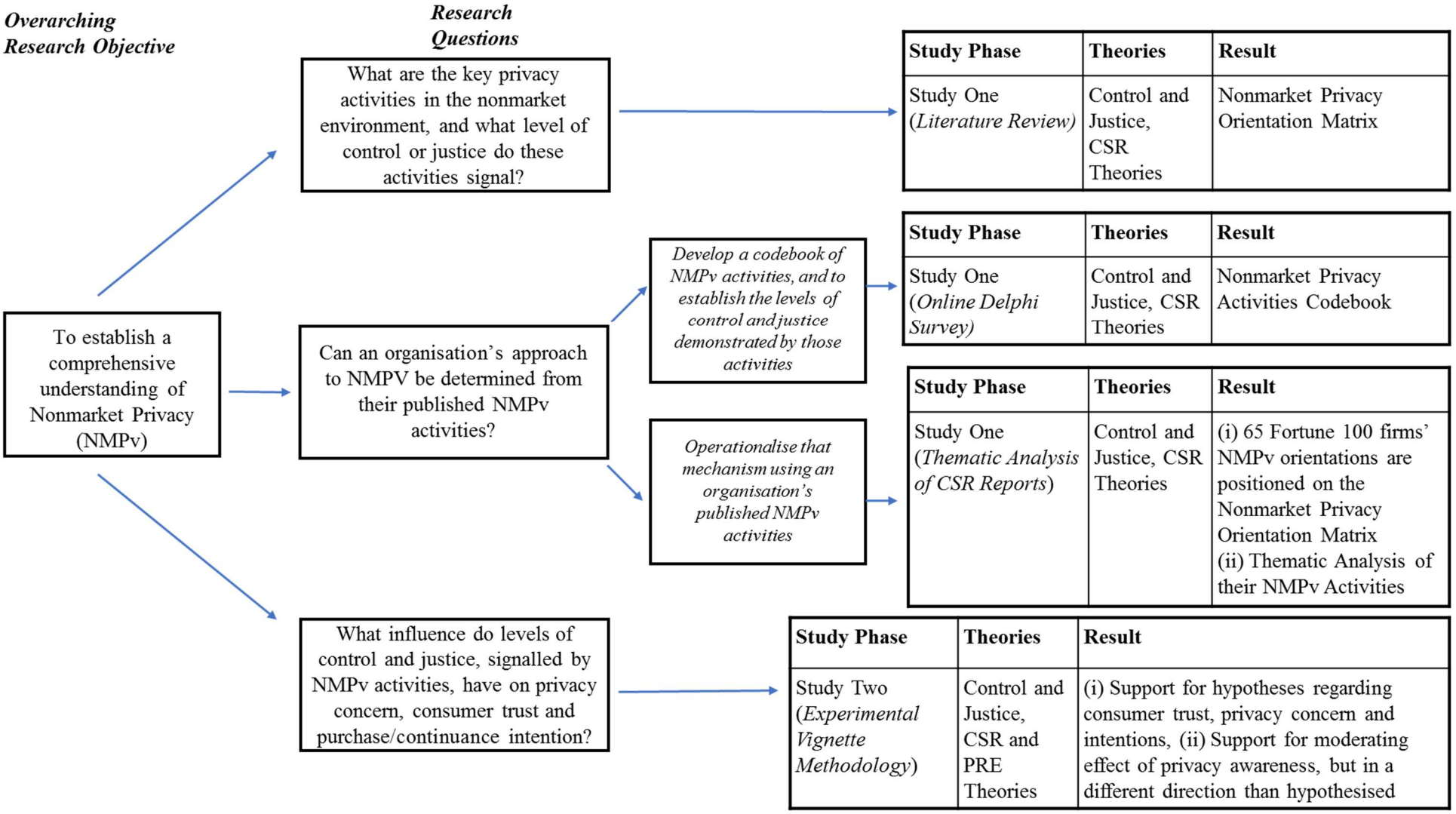


Figure 7.1 Visualisation of the Research

7.2 Discussion of Key Findings

In Study One, a framework of NMPv approaches is constructed, characterised by levels of control and justice. This framework is called the Nonmarket Privacy Orientations Matrix. A codebook of associated NMPv activities, also characterised by levels of control and justice, is constructed. The codebook is called the Nonmarket Privacy Activities Codebook. The codebook is applied to a number of CSR publications (*n=65*) to position their approach to NMPv in one of the primary orientations of the Nonmarket Privacy Orientation Matrix. Study One finds that whilst most organisations conduct NMPv activities, the majority continue to focus on compliance, and are positioned in the Risk Management NMPv orientation. However Study One also finds that many of the organisations from the technology and telecommunications industry, are positioned in the justice-based orientations of Citizenship and Warrior, and report justice-based NMPv activities exceeding regulation. This is important as studies have found that organisations exceeding privacy regulation experience less privacy breaches (Accenture and Ponemon Institute, 2015; Culnan and Williams, 2009).

Continuing the investigation of control and justice in NMPv, Study Two investigates the relationship between levels of control and justice signalled by an organisation's NMPv activities, and privacy concern, consumer trust and purchase intention/continuance intention. Leveraging PRE theory (Davis et al., 1980), and building on the PRE Model of Privacy (Lwin et al., 2007), a theoretical research framework is constructed to test the hypothesised relationships. Study Two finds that control-based NMPv activities have a negative influence on consumer trust and purchase intention/continuance intention, and a positive influence on privacy concern. Whereas justice-based NMPv activities have a positive influence on consumer trust and purchase intention/continuance intention, and a negative influence on privacy concern.

The remainder of this section presents the findings of both studies in this research.

7.2.1 Study One: Key Findings

Study One addresses RQ1 and RQ2, by developing a framework that explains organisational approaches to NMPv and their associated activities, and developing a mechanism that can position an organisation's approach to NMPv. The following section discusses the key results for RQ1 and RQ2.

7.2.1.1 A Framework of Nonmarket Privacy Approaches

To establish a foundational understanding of approaches to NMPv, a critical literature review across the business ethics, information systems, and nonmarket environment literature was conducted. NMPv emerged as a relatively unexplored phenomenon. Whilst a growing interest in privacy as a CSR (e.g., Lobschat et al.,2021; Martin, 2020, Schultz and Seele, 2019) emerged in the business ethics literature, a paucity of research investigating Corporate Political Privacy or Sociopolitical Privacy was evident. The inclusion of all three NMPv strategies is important, as all three affect an organisation's bottom line (Bhagwat et al., 2020; Chernev and Blair, 2015; Hillman and Hitt, 1999).

In order to develop a theoretical framework of organisational approaches to NMPv, the IS literature provided a starting point, in the form of the CIPO model from Greenaway et al. (2015). In CIPO, Greenaway et al. (2015) combined theories of control and justice to explain how organisations' privacy policies affect their customers' abilities to exercise control and justice mechanisms over the processing of their personal information. Their use of control and justice theory to explore privacy in this way, forms the starting point for this research. Dimensions of CIPO do not address social and political aspects of privacy however, therefore this research incorporates social and political dimensions by leveraging current approaches to nonmarket strategy, namely CSR Postures from Castello and Lozano (2009) and CSR Generations (Trapp, 2012). Characterised by control and justice, this research posits the existence of four approaches to NMPv, in a framework called the

Nonmarket Privacy Orientation Matrix. These approaches to NMPv are described as (i) the Risk Management NMPv Orientation, (ii) the Integrated NMPv Orientation, (iii) the Citizenship NMPv Orientation, and (iv) the Warrior NMPv Orientation.

Whilst researchers recognise the importance of nonmarket environment orientations (Castello and Lozano, 2009), they have yet to recognise the importance of these orientations in the context of privacy activities in the nonmarket environment. A significant contribution of this research is the conceptualisation of approaches to NMPv in this way, thus enabling insight and a deeper understanding of the phenomenon. As nonmarket strategies can result in positive performance outcomes such as firm reputation, consumer trust, and long-term loyalty (Chernev and Blair, 2015; Homburg et al., 2013), it seems likely that privacy-specific nonmarket strategies could experience similar outcomes.

7.2.1.2 Determining Nonmarket Privacy Orientations

Responding to calls from Greenaway et al. (2015), the second objective of this research aimed to construct a mechanism that could determine levels of control and justice that are signalled by an organisation's NMPv activities, and to use that mechanism to position an organisation's NMPv orientation. Leveraging the Online Delphi Survey method, a panel of privacy experts categorised and weighted a set of control-based NMPv activities and justice-based NMPv activities, to form the Nonmarket Privacy Activities Codebook. Following this, the Nonmarket Privacy Activities Codebook was systematically applied, using the matrix approach to thematic analysis (Groenland, 2018), to sixty-five CSR reports from the Fortune 100 index. Each of the organisation's NMPv orientations were then determined.

The Risk Management NMPv orientation was found to be the most common. Only Best Buy and General Motors were positioned in the Integrated NMPv orientation, and only AT&T and Verizon were positioned in the Citizenship NMPv orientation, notably both

from the Telecommunications industry. Six organisations were positioned in the Warrior NMPv orientation: Allstate, Apple, Cisco, IBM, HP, Microsoft, all of which were from the Technology industry except Allstate. The thematic analysis also provided a deeper understanding of the NMPv activities undertaken by these organisations. More than seventy-five percent of the organisations reported control-based NMPv activities, including all the organisations in the high-justice NMPv orientations. This confirms assertions from Hughes (2012) that organisations must exercise some level of control over information in order to provide compliance. However, similar to findings from Pollach (2011), few organisations exceeded compliance. Forty-one percent of organisations positioned in the Risk Management NMPv orientation were found to report little beyond compliance-related NMPv activities. This supports assertions of the Nonmarket Privacy Orientation Matrix that organisations in the low-justice NMPv orientations will focus on simple compliance. In contrast, NMPv activities exceeding regulation were reported by all organisations in the high-justice NMPv orientations *(n=8)*. The key findings of Study One are discussed below for each NMPv strategy, namely Corporate Social Privacy, Corporate Political Privacy and Sociopolitical Privacy.

Corporate Social Privacy

All of the organisations positioned in the Integrated, Warrior and Citizenship NMPv orientations *(n=10)* reported NMPv activities exceeding regulatory minimums, however the high-justice NMPv orientations reported more of these than the low-justice NMPv orientations. Justice-based privacy activities are important because when organisations fail to promote justice in their privacy activities, consumers react negatively and their privacy concern increases (Lwin et al., 2007). Accordingly, when consumers perceive that organisations are acting responsibly in their NMPv activities, consumers show less concern for privacy and reduce potentially damaging negative consumer responses. This would suggest that high-justice NMP orientations would engender less concern for privacy and

more positive consumer responses than low-justice NMPv orientations. This is notable, as preliminary evidence from industry reports suggest that organisations who protect information in a way that exceeds regulatory compliance experience less privacy incidents (Accenture and Ponemon Institute, 2015). In this way, organisations in high-justice NMPv orientations would be expected to experience less privacy incidents.

The Nonmarket Privacy Orientation Matrix asserts that organisations in the low-justice NMPv orientations conduct little more than control-based NMPv activities, e.g., compliance. Organisations in the Integrated NMP orientation are more aware of society's evolving privacy expectations, and relationships with stakeholders evolve from one-way communication to dialogue and collaboration (Castello and Lozano, 2009). Supporting these assertions, organisations in the Risk Management NMPv orientation reported little beyond compliance, whereas Corporate Social Privacy became more evident in the Integrated NMPv orientation and beyond, where organisations began to report privacy as an issue concerning multiple stakeholders, and reported justice-based privacy activities involving collaborations with multiple privacy advocacy groups. This is important, as nonmarket activities that reflect values of justice are associated with signalling integrity (Park et al., 2014) and benevolence (Hess, 1995). A breach of justice in these dimensions can lead to reduced consumer trust and purchase intentions (Bansal and Zahedi, 2015). Therefore high-justice NMPv orientations i.e., those that conduct Corporate Social Privacy activities, are more likely to engender consumer trust and purchase intentions than low-justice NMPv orientations.

The Nonmarket Privacy Orientation Matrix asserts that the high-justice NMPv orientations focus on building and maintaining strategic and sustainable relationships. In the high-justice NMPv orientations, organisations form long-term alliances with stakeholders to drive changes in social issues (Trapp, 2012). Eighty-seven percent of organisations categorised in the Warrior and Citizenship NMPv orientation ($n=7$), reported NMPv

activities involving collaborations with advocacy groups. Only twenty-five percent (*n=13*) of organisations categorised in the Risk Management NMPv orientation reported this type of activity. This is important, as cooperative relationships in the nonmarket environment are argued to reduce the threat of agent/stakeholder opportunism and generate competitive advantages associated with mobilising joint learning capabilities (Jones, 1995). Notably, organisations in the low-justice NMPv orientations reported collaborations in a way that benefitted themselves or their immediate stakeholders, where organisations in the high-justice NMPv orientations reported collaborations with organisations in a way that advocated for strengthened privacy for society.

The Nonmarket Privacy Orientation Matrix asserts that organisations in the high-justice NMPv orientations assign responsibility for privacy to the C-Suite, which is a Corporate Social Privacy activity. The findings in this research support this assertion, as the organisations in the high-justice NMPv orientations reported such an appointment, most notably all the technology sector organisations, except for Dell and Oracle. Privacy at the C-Suite level was most often represented by the appointment of a Chief Privacy Officer (CPO). Appointing any role to the C-Suite level is a strategic action that sends signals to both internal and external stakeholders about the strategic importance of a role (Weingarten et al., 2017). The appointment of a CPO can also help the organisation to connect with external stakeholders, to obtain more external resources, and improve its reputation (Bamberger and Mulligan, 2011). In this way, organisations can deepen the involvement of top management in privacy stewardship rather than simple leadership (Caldwell et al., 2010), supporting assertions of the Nonmarket Privacy Orientation Matrix that privacy stewardship is evident in the high-justice NMPv orientations.

Corporate Political Privacy

An organisation's basic approach to CPA is determined by its implicit view of the nature of citizenship, where instrumental approaches are congruent with a liberal minimalist understanding of citizenship, and cooperative approaches are congruent with a competent partnership understanding of citizenship (Anastasiadis, 2014). Corporate Political Privacy activities reflecting the instrumental approach were classified in the Nonmarket Privacy Activities Codebook as a control-based NMPv activity i.e., lobbying that benefitted the organisation. Whereas Corporate Political Privacy activities reflecting the cooperative approach were classified in the Nonmarket Privacy Activities Codebook as a justice-based NMPv activity, i.e., lobbying that benefitted consumers or society.

The Nonmarket Privacy Orientation Matrix asserts that organisations in the low-justice NMPv orientations will conduct Corporate Political Privacy in a way that reflects the instrumental approach and benefits themselves, where organisations in the high-justice NMPv orientations will conduct Corporate Political Privacy in a way that reflects the partnership approach and favours consumers or society. Supporting these assertions, this research found that justice-based Corporate Political Privacy was reported by organisations in the high-justice NMPv orientations, and control-based Corporate Political Privacy was reported by organisations in the low-justice NMPv orientations. This is important as partnership approaches to Corporate Political Privacy consider the needs of a wider range of stakeholders. These partnership approaches emphasise the adoption of prosocial values and behaviours and socially contracted relationships (Caldwell and Karri, 2005), extending beyond the organisation to other levels of society such as the industry or community (Hernandez, 2012). This type of Corporate Political Privacy aligns closer to the altruistic values of CSR (Lock and Seele, 2017) and is more likely as a result to engender benevolence, a key dimension of trustworthiness, as benevolence is associated more with CSR than CPA (DenHond et al., 2014). It would also be expected the Corporate Political

Privacy undertaken in the high-justice orientations would result in other benefits associated with CSR such as increased consumer loyalty and reduced firm risk (Glaveli, 2020) and such an investigation would present a fruitful avenue for future research.

Only four organisations reported Corporate Political Privacy in their CSR reports. Given this number, wider generalisation of these findings is difficult. This also suggests that most organisations do not frame Corporate Political Privacy as part of their nonmarket agenda, and would reflect earlier assertions of the researcher regarding how the literature had associated privacy with CSR but had not yet associated privacy as a CPA or SPI. For example, Google, who is positioned in the Risk Management NMPv orientation, has conducted Corporate Political Privacy activities that are more favourable to itself than the consumer, however it has not reported this Corporate Political Privacy in their CSR report. Whilst this supports assertions in the Nonmarket Privacy Orientation Matrix regarding the type of Corporate Political Privacy conducted in different NMPv orientations, this presents a limitation associated with using just CSR publications. Extending the search for Corporate Political Privacy to media reports and lobbying databases would address this limitation and present an interesting avenue for future research.

Sociopolitical Privacy

Although SPI is related to CSR and CPA, it is a nascent and emergent construct that has yet to be clearly elucidated, and is a relatively new phenomenon (Bhagwat et al., 2020; Hambrick and Wowak, 2021). Whilst it is evident that Sociopolitical Privacy is an activity being undertaken by some large organisations, such as those in the sample in Study One, it is not reported as part of their nonmarket agenda. Therefore, with the exception of Cisco, who reported on its partisan position regarding government use of technology to curtail freedom of expression, there was little Sociopolitical Privacy reported in the CSR publications. However a search of media reports found that three organisations in the

Warrior NMPv orientation (Apple, Cisco and Microsoft) together with both organisations in the Citizenship NMPv orientation (AT&T and Verizon) were found to have filed amicus briefs appealing the U.S. law enforcement decision to force Microsoft to hand over data about an Irish customer (Microsoft, 2020). Apple was also found to have challenged at least 12 orders issued by the FBI compelling Apple to enable decryption of phones involved in criminal investigations and prosecutions (PEW Research Centre, 2016). Future research could explore organisations' Sociopolitical Privacy activities published in the media/press, and thus expand our knowledge and understanding of this rather nascent NMPv activity.

7.2.2 Study Two: Key Findings

Responding to the third RQ required an understanding of the relationship between the levels of control and justice signalled by an organisation's NMPv activities and privacy concern, consumer trust and purchase intention/continuance intention. This section discusses the key findings from Study Two, and is followed by a presentation of the revised research model, based on those findings.

It was hypothesised that control-based NMPv activity would negatively influence consumer trust and purchase intention/continuance intention and positively influence privacy concern. It was also hypothesised that justice-based NMPv activity would positively influence consumer trust and purchase intention/continuance intention, and negatively influence privacy concern. The results in both experiments provide support for these hypotheses. Control-based NMPv activity is found to result in higher privacy concern, and less consumer trust and purchase intention/continuance intention, than justice-based NMPv activity. Thus, the results from Study Two extends support for existing studies on the influence of control on increasing privacy concern (Pavlou and Fygenson, 2006; Phelps et al., 2000; Xu, 2007) to the nonmarket context. These results

also extend support in existing studies for the influence of justice on the relationship between an organisation's privacy activity and reducing privacy concern (Bandara et al., 2020; Culnan and Armstrong, 1999; Culnan and Bies, 2003; Greenaway et al., 2015; Lwin et al., 2007) to the nonmarket environment context. The results also extend support in existing studies, for the influence of justice on the relationship between an organisation's privacy activity and consumer trust (Bansal et al., 2008; Hong and Thong, 2013; Malhotra et al., 2004; Miltgen and Peyrat-Guillard, 2014) and the consumer's intentions (Fang et al., 2011), to the nonmarket context. The research also found that justice-based Corporate Political Privacy e.g., lobbying for privacy so as to benefit the consumer and/or society, was associated with less privacy concern than justice-based Corporate Social Privacy, and was also associated with increased continuance intention.

It was also hypothesised that a consumer's level of privacy awareness would moderate how NMPv activities influence privacy concern, consumer trust and continuance intention. In other words, a consumer's understanding of their own privacy rights, or of an organisation's privacy obligations, would influence the strength of the relationship between NMPv activity and consumer responses. Privacy awareness was found to have no significant moderating effect on the relationship between NMPv activities and privacy concern. Whilst it was hypothesised that the relationship between NMPv activities and both consumer trust and continuance intention is negatively moderated by privacy awareness, this research found the opposite. The positive effect of NMPv activities on consumer trust was strongest for consumers who had high privacy awareness. Similarly, the positive effect of NMPv activities on continuance intention was strongest for consumers who had high privacy awareness. There are a number of suggested explanations for this. First, as noted in Section 3.4.1., previous studies have found a lack of privacy literacy among consumers, where many cannot understand the breadth of their privacy rights across multiple jurisdictions, nor understand the breadth of organisation's privacy

obligations across (Proton Technologies, 2019). Second, and related to the first, this research leveraged a series of measures for privacy awareness from Warner and Wang (2019) that were based on self-disclosure. These measures do not examine true awareness levels. The third possible explanation, again related to the previous two, is "privacy cynicism". Privacy cynicism is a coping mechanism that allows low-skilled users to ignore privacy concerns and engage in online activity or disclosure without increasing privacy protection behaviours (Hoffman et al., 2016). In summary, in this research it was expected that high privacy awareness would result in, for instance, a strengthened negative relationship between NMPv activity and continuance intention, where consumers with high levels of privacy awareness would respond to NMPv activity with decreased continuance intention. However, where individuals have mistakenly self-disclosed as having high privacy awareness levels, they may not really understand the complexities of privacy legislation, or some individuals with low privacy awareness may have high privacy cynicism.

Finally, in Experiment 2, perceived need for government surveillance was included as a control variable (Dinev et al., 2008) and was found to account for a significant amount of variance (10%) in both consumer trust and continuance intention but not privacy concern. This would indicate that perceived need for government surveillance has a predictive influence on consumer trust and continuance intention, and further research could explore these effects. Existing studies find that perceived need for government surveillance negatively influences privacy concern (Dinev et al., 2008; Dinev et al., 2009; Thompson et al., 2020) however this could not be supported in this research. Future research could thus investigate the influence of perceived need for government surveillance on the relationship between NMPv activities and these consumer outcomes.

7.3 Towards a Revised Framework

The research framework in this thesis provides a gateway to deeper research into the relationship between NMPv activities, and their influence on the consumer. This is important because NMPv activities are clearly conducted by organisations, but with little guidance on the influence that certain NMPv strategies and associated NMPv activities have on consumer trust, privacy concern and purchase intention/continuance intention. Organisations may thus be undertaking NMPv activities that negatively impact the consumer and their responses, or they may be missing opportunities to engage with NMPv activities that more positively impact the consumer and their responses. The underlying theoretical assumptions and constructs in the framework, developed for this research, are briefly summarised below.

Building on the PRE Model of Privacy (Lwin et al., 2007), the research framework developed in this thesis proposes that certain consumer responses are shaped by levels of control and justice signalled by an organisation's privacy activities in the nonmarket environment, together with personal characteristics of the consumer. The literature already provides support for these relationships in the traditional privacy context, for example, between privacy statements and privacy concern (Wu et al., 2012), between privacy policies and consumer trust (Mutimukwe et al., 2020; Milne and Culnan, 2004) and between privacy policies and purchase intention (Tsai et al., 2010). To the researcher's knowledge, this is one of the first studies to extend support for these relationships to the nonmarket context.

The research framework, initially presented in Chapter Three, was revised to reflect the results of this research and is presented in Figure 7.2. This framework can be retested and further advanced to develop a more comprehensive understanding of privacy in the nonmarket context. The revised framework positions the NMPv orientation and associated NMPv activities, as outcomes of an organisation's NMPv strategies i.e., Corporate Social

Privacy, Corporate Political Privacy or Sociopolitical Privacy. NMPv activities are also positioned as the 'interaction' between the levels of control and justice signalled by an organisation's NMPv strategies and consumer responses. As individual characteristics and personal attitudes have been found to influence both privacy concern (Malhotra et al., 2004; Smith et al.,1996) and consumer trust (Mezger et al., 2020), they are included as control variables. Whilst privacy awareness was found to moderate the relationship between NMPv activities and consumer trust and purchase intention/continuance intention, it was not found to moderate the relationship with privacy concern, and therefore the research framework was amended to reflect this.

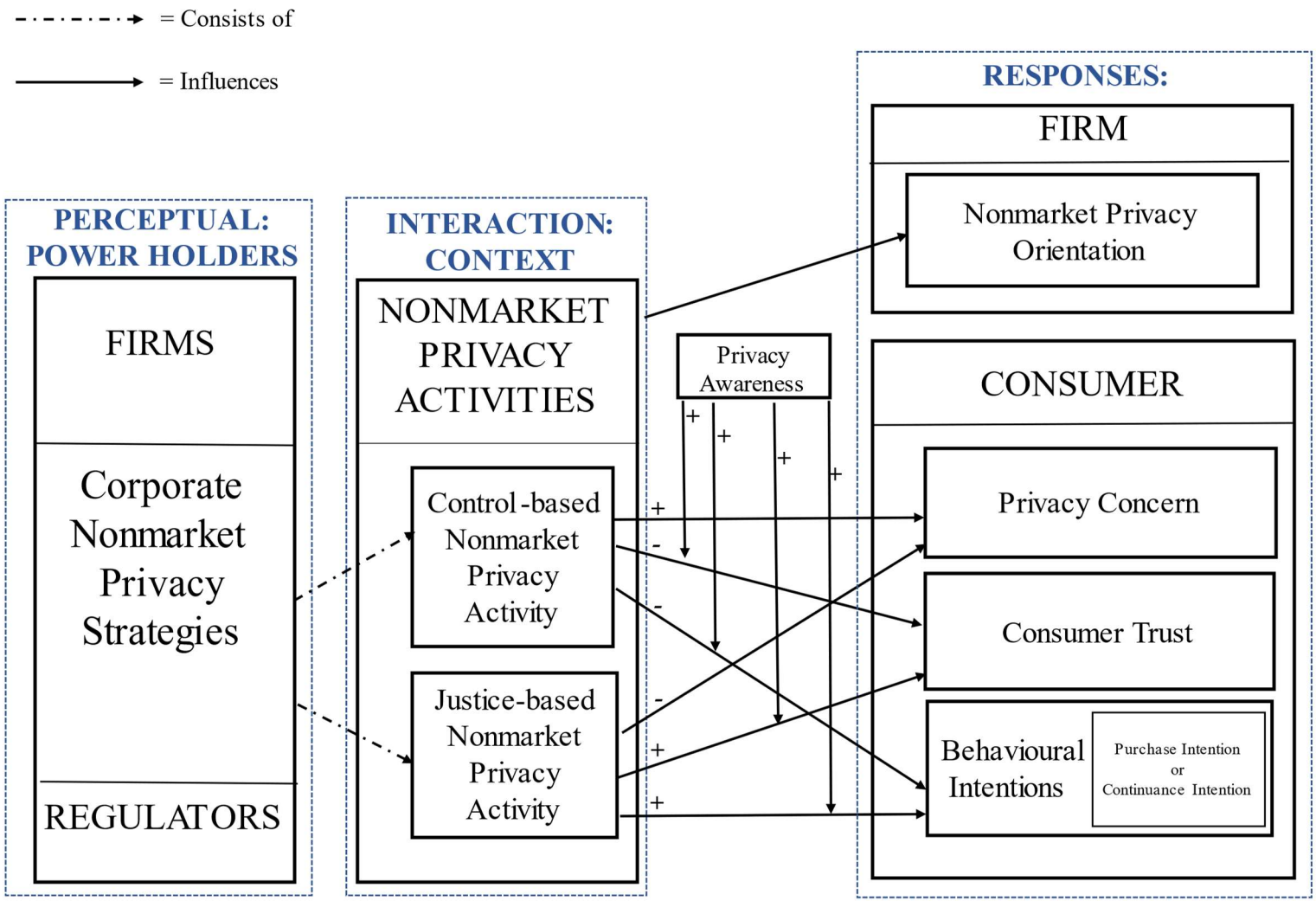


Figure 7.2 A Revised Framework

7.4 Research Contributions

The importance of privacy to a functioning society has been widely discussed in the literature (Rachels, 1975; Moradian, 2009). The importance of the nonmarket environment to firm performance has also been widely discussed (Wiengarten et al., 2019; Wiengarten et al., 2012). The researcher integrates theories of the nonmarket with theories of privacy, in order to establish an innovative approach to privacy that can encourage organisations to be less focused on addressing privacy as a legal requirement i.e., 'doing privacy rights', and to be more focused on addressing privacy as a societal value i.e., 'doing privacy right'.

In the business and ethics literature, the IS literature and the nonmarket literature, privacy in the nonmarket environment remained a relatively unexplored phenomenon. However, the number of Fortune 100 organisations who are already reporting NMPv activity has been steadily rising since 2015 (Forrester, 2018). Due to the lack of research into this phenomenon, organisations are potentially undertaking NMPv activities without a comprehensive understanding of the positive and negative influence that such activities may have on their consumers and on the wider stakeholder community. This research aims to fill this gap, and sets out to deepen our understanding of privacy in the nonmarket environment. The overarching contribution of the research is the exploration of an important, yet relatively unexplored phenomenon. This research makes a number of unique contributions. These contributions are discussed in the remainder of this section, where contributions to knowledge are first discussed, then implications for practice and policymakers are discussed.

7.4.1 Contribution to Knowledge

Theory usually begins with a research question, together with a number of more 'craftsmanship-level' aspects of a theory where contributions can be made i.e., the mode of theorizing, the level of analysis, an understanding of the underlying phenomenon, causal

mechanisms, constructs and variables, and boundary conditions (Makadok et al., 2018). Based on headings used by Makadok et al. (2018), this section presents the contributions to theory under the following four headings; (i) introducing a previously overlooked or new phenomenon, (ii) expanding a current model, (iii) applying an existing theory to a different phenomenon or context, and (iv) devising new outputs from combining theories. The contributions to theory are summarised in Table 7.1.

Table 7.1 Summary of the Key Contributions to Knowledge in this Research

Contribution Category	Contribution
Introducing a previously overlooked or new phenomenon.	• Privacy as a nonmarket environment strategy. • A taxonomy of nonmarket privacy. • The Nonmarket Privacy Orientation Matrix. • The Nonmarket Privacy Activities Codebook.
Expanding a current model.	• This research is the first to interpret responsibility as justice and power as control, in the context of the PRE theory. This extends application of the PRE Model of Privacy (Lwin et al., 2007), to explore the equilibrium between control and justice in future privacy research. • Expanding outcomes of the PRE Model of Privacy to include consumer trust and intention to purchase a product or service, or to continue use of an IS system. • Current dimensions of CIPO (Greenaway et al., 2015) are information strategy, legal and ethical dimensions. This research expands CIPO to include societal expectations as an additional dimension. • Extends contextual factors of the APCO model (Smith et al., 2011) to include CSR reports as 'privacy interventions', and extends macro factors of the APCO model to include an organisation's responsible, political and sociopolitical NMPv strategies, i.e., Corporate Social Privacy, Corporate Political Privacy and Sociopolitical Privacy.

Contribution Category	Contribution
Applying an existing theory to a different phenomenon or context	• Applying PRE theory to privacy i.e., the PRE Model of Privacy (Lwin et al., 2007) in the nonmarket environment context, to test the influence that levels of control and justice in NMPv activities have on consumers. • Applying current control and justice approaches to privacy i.e., the Company Information Privacy Orientation model (Greenaway et al., 2015), but in the nonmarket environment context, to explain how control and justice influence nonmarket privacy orientations i.e., the Nonmarket Privacy Orientation Matrix. • Applying CSR Posture theory (Castello and Lozano, 2009), used to explain approaches to nonmarket strategy, to the context of privacy for the first time, in order to explain approaches to nonmarket privacy.
Devising new outputs from combining theories.	• By combining perspectives of privacy and the nonmarket environment over four decades, a set of perspectives of privacy in the nonmarket environment emerge, that explain a progression of privacy thinking, previously not described. • By combining nonmarket strategies (CSR, CPA, SPI) with privacy, a set of nonmarket privacy strategies are presented i.e., Corporate Social Privacy, Corporate Political Privacy, Sociopolitical Privacy, together with a set of associated nonmarket privacy activities. • By combining current approaches to privacy i.e., CIPO from Greenaway et al. (2015) with approaches to CSR i.e., CSR Postures from Castello and Lozano (2009), a set of four approaches to nonmarket privacy are presented as the Nonmarket Privacy Orientations Matrix. • By combining privacy with the nonmarket environment, the researcher asserts that privacy can engender benefits associated with the nonmarket environment, such as increased consumer trust and brand loyalty (Glaveli, 2020), and extends these benefits to include reduced privacy concerns.

7.4.1.1 Introducing a Previously Overlooked/New Phenomenon

Whilst privacy has been referred to as a CSR (e.g., Flyverbom et al., 2019; Howe and Nisenbaum, 2009; Martin, 2016; Scherer, 2018), there is still a paucity of research exploring privacy as a CSR (Allen and Peloza, 2015; Pollach, 2011). More recently, several articles have emerged in business and ethics research referring to privacy as a CSR (e.g., Bandara et al., 2020; Lobschat et al., 2021; Martin, 2020; Shilton and Greene, 2019) indicating that privacy as a CSR has become a topic of scholarly discourse in the business and ethics domain. However, the literature has failed to explore privacy through the lens of other important nonmarket strategies such as CPA or SPI, despite organisations investing heavily in political activities aimed at controlling and shaping privacy. This research adds to the current discourse, and extends its reach to both the IS and nonmarket literature. Whilst the literature referencing privacy in the nonmarket environment is increasing, NMPv has not been widely recognised as a means by which organisations can enhance stakeholder relationships (Allen and Peloza, 2015). This research addresses this gap, by highlighting the NMPv activities that can positively influence the consumer relationship, and the NMPv activities that can damage the relationship.

In describing and exploring three key nonmarket privacy strategies as Corporate Social Privacy, Corporate Political Privacy, and Sociopolitical Privacy, this research establishes a typology for privacy in the nonmarket context, not previously discussed in the literature. In this way, this research establishes a common language for future dialogue and research regarding NMPv. Figure 7.3 presents a summary of the typology for privacy in the nonmarket environment, as established throughout this research.

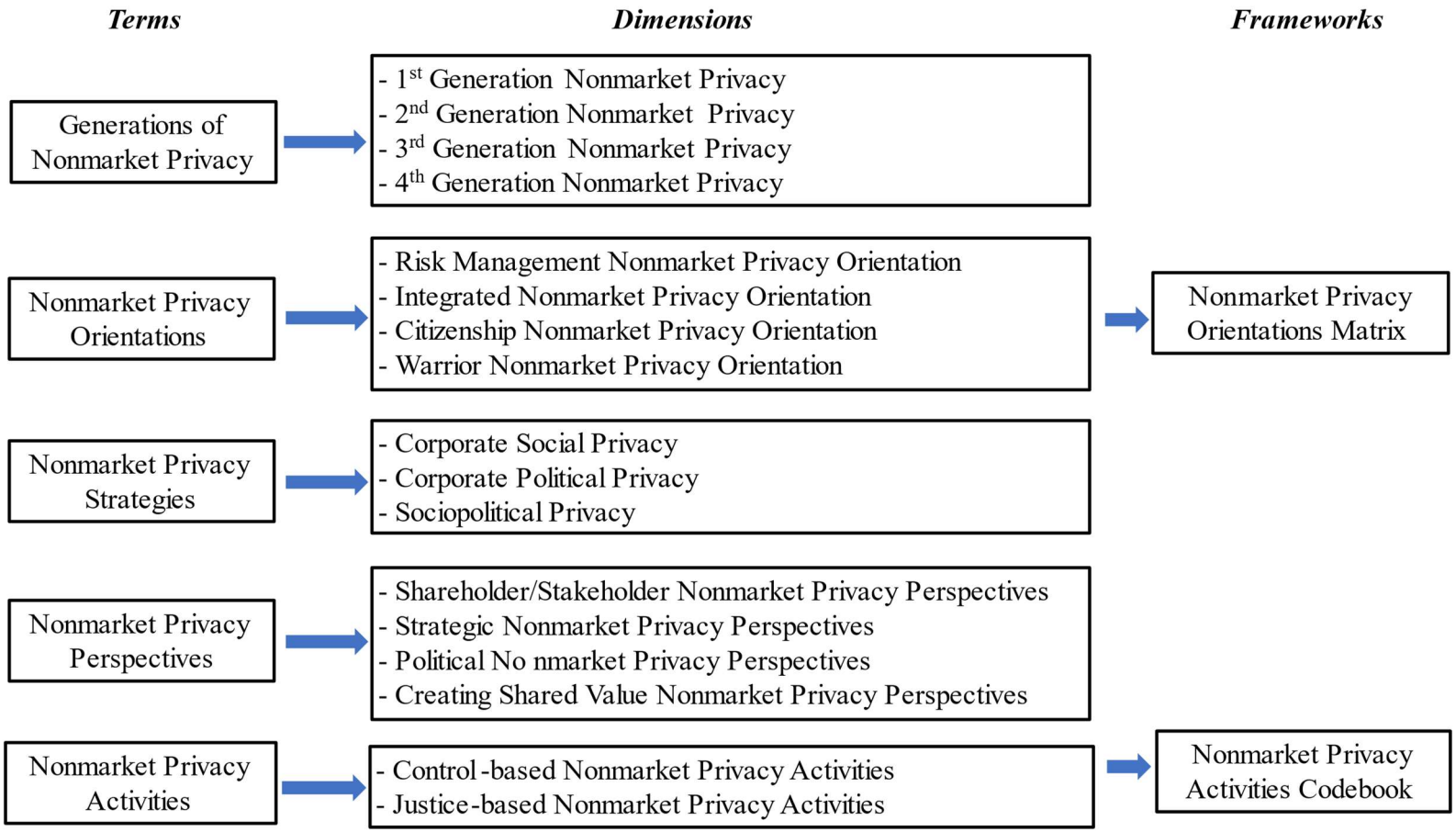


Figure 7.3 Summary Typology of Nonmarket Privacy

7.4.1.2 Expanding a Current Model

PRE has been identified as a useful ethical and social responsibility approach to investigate consumer privacy issues (Bandara et al., 2020; Krishen et al., 2017; Martin and Murphy, 2017). However, its empirical application in the privacy context remains largely limited (i.e., Bandara et al., 2020; Krishen et al., 2017; Lwin et al., 2007). The PRE Model of Privacy (Lwin et al., 2007) does not include individual characteristics important to privacy such as an individual's propensity to trust, their disposition to value privacy, their attitudes towards government surveillance, and their political affiliation. By providing empirical support and in-depth insights into the influence these factors have on privacy related consumer outcomes in this research, the researcher proposes extending the PRE Model of Privacy (Lwin et al., 2007) to include these factors. In the PRE Model of Privacy (Lwin et al., 2007), consumer responses are elucidated as Fabricate, Protect, Withhold. However, this research extends these responses to also include the consumer's intention to purchase or continue use of a system. Including intentions is important as intentions are the most influential predictor of a consumer's actual behaviour (Ajzen, 1991), and are associated as responses to privacy concern (Fortes and Rita, 2016) or responses to consumer trust (e.g., Kim et al., 2009, Kim et al., 2010, Liao et al., 2011).

Previous studies have extended the PRE Model of Privacy to include constructs related to consumer control, e.g., Bandara et al. (2020) included 'privacy empowerment' and Krishen et al. (2017) included 'internal locus of control'. As previously noted however, control is a shared responsibility that cannot be exercised by the consumer alone, without the organisation putting an architecture of control in place, such as a regulated set of structural measures that aim to secure an individual's personal data (Lazaro and Le Metayer, 2015). This research therefore includes both control and justice in order to reflect the tensions between the organisation's need for control and the consumer's need for control.

Whilst the formation of an organisation's CIPO is based on how an organisation reconciles its information management, ethical and legal obligations (Greenaway et al., 2015), by rooting this research in theories of Corporate Social Responsibility, this research proposes that the formation of an organisation's NMPv orientation extends beyond this, to include reconciling the complex interconnection between an organisation's core activity and the greater global context of privacy. As such, the formation of an organisation's NMPv Orientation also includes the organisation's roles and responsibilities towards society with regard to privacy. In this way, this research extends the dimensions forming CIPO to also include reconciling the organisation's roles and responsibilities towards society with regard to privacy with its information management, ethical and legal obligations.

The researcher proposes an extension to CSR postures from Castello and Lozano (2009), referring to this additional posture as the Warrior CSR Posture. The Warrior CSR Posture adopts a revolutionist approach to nonmarket activities. Such an approach can include participation in protests, breaching laws, and even alienating certain stakeholders in order to address social issues such as privacy. The researcher also extends existing conceptualisations of the evolution of CSR from Trapp (2012) called CSR Generations. The researcher also extends Generations of CSR from Trapp (2012) to include a Fourth Generation CSR. In Fourth Generation CSR, organisations not only spearhead social change, but demonstrate commitment to certain social values to the extent they will breach laws. These additional postures and generations have most likely evolved in response to the previous noted changing societal expectations towards organisations (Johnson, 2019), or could be the result of the changing attributes of leadership (McKinsey, 2019). These postures are important to understand, as organisations sometimes take a value-based position on social matters that result in their breaching legislation.

In the IS literature on privacy, the APCO model from Smith et al. (2011) provides a useful way to summarise the previous scholarly work regarding antecedents to, and outcomes of,

privacy concern (Miltgen and Peyrat-Guillard, 2014). Individual factors, contextual factors, and macro factors are modelled in the APCO model as antecedents. Beliefs and behaviours are modelled in the APCO model as outcomes. Responding to calls for deeper consideration of macro and contextual factors (Miltgen and Peyrat-Guillard, 2014), this research extends contextual factors of the APCO model to include CSR reports as 'privacy interventions', and extends macro factors of the APCO model to include an organisation's responsible, political and sociopolitical NMPv strategies, i.e., Corporate Social Privacy, Corporate Political Privacy and Sociopolitical Privacy. This is important, as this research finds that many organisations are actively engaging with these NMPv strategies, and finds that these strategies influence privacy concern.

7.4.1.3 Applying an Existing Theory(s) to a Different Phenomenon or Context

Applying Control and Justice (CIPO) to the Nonmarket Environment Context

In the existing information privacy literature, several studies have explored the influence of either control or justice on privacy concern, consumer trust and purchase intention/continuance intention, across various contexts, e.g., Culnan and Bies (2003), Bansal and Zahedi (2015), and Lwin et al. (2007). However only Greenaway et al. (2015) explore privacy by combining both control and justice theories, to form a conceptual model called CIPO. Mirroring their application of control and justice as a starting point, this research is the first to conceptualise NMPv orientations in the Nonmarket Privacy Orientation Matrix.

Combining control and justice is important, as in any information exchange relationship there are often opposing forces at play regarding privacy (for example, between employee-employer, citizen-government, consumer-business, patient-hospital, student-university, and so on). Therefore, a one-sided lens cannot truly represent the tensions arising from privacy between multiple constituents, jurisdictions, stakeholders, and contexts (Hughes, 2012).

Additionally, control is a shared responsibility that cannot be exercised by the consumer alone without the organisation putting an architecture of control in place, such as a regulated set of structural measures that aim to secure an individual's personal data, namely technological controls and organisational controls (Lazaro and Le Metayer, 2015). By combining control and justice, this research also provides empirical support for the relationship between levels of control and justice signalled by an organisation's NMPv activity and outcomes for consumers. For instance, justice-based NMPv activities are more likely, than control-based, to positively shape a consumer's perceptions of an organisation, and result in benefits typically associated with nonmarket environment activities, such as increased stakeholder trust and loyalty (Glaveli, 2020). This is important as understanding these influences enables organisations to better predict the effect their NMPv activities may have on their consumers and their wider stakeholder audience in the future.

Applying PRE Theory to the Nonmarket Environment Context

Power has been acknowledged in nonmarket scholarship as having critical importance in both CSR (e.g., Banerjee, 2008; Bondy, 2008) and CPA (e.g., Frynas et al., 2017). Responding to calls from Frynas et al. (2017) for more power-based approaches to nonmarket environment research, this research takes a power-based approach to NMPv research, using PRE theory. Whilst PRE theory has been used previously in both nonmarket scholarship (Liedong et al., 2014) and privacy scholarship (Bandara et al., 2020; Krishen et al., 2017; Lwin et al., 2007), this research builds on and extends application of PRE theory to the context of NMPv. This is important, as a power-based approach to research has been identified as a useful ethical and social responsibility approach to investigate privacy (Krishen et al., 2017; Martin and Murphy, 2017) and to investigate nonmarket strategies (Frynas et al., 2017).

In this research, the research framework interprets NMPv activities that express power and influence over data as control-based activities, and interprets NMPv activities that express responsibility as justice-based activities. In this way, power and responsibility are characterised by levels of control and justice signalled by the privacy activities of the organisation's nonmarket strategies and associated activities. Organisations can overstep acceptable levels of control by not demonstrating responsible use of information, or by undertaking NMPv activities in a way that benefits the organisation and disenfranchises the consumer. For instance, organisations could lobby the government for reduced privacy rights for consumers. This research thus extends the applicability of the PRE Model of Privacy (Lwin et al., 2007) to explore an organisation's privacy activities in terms of power and responsibility OR in terms of control and justice. To the best knowledge of the researcher, this research is the first to interpret power and responsibility of PRE theory (Davis et al.,1980; Laczniak and Murphy, 1993; Murphy et al., 2005) in this way, as control and justice. The findings in this research support the assumptions underlying the PRE Model of Privacy (Lwin et al., 2007) that power and responsibility, i.e., control and justice, need to be in balance in order to provide sustainability. This research is the first to advance the use of power-based approaches to investigate the phenomenon of NMPv. However, it further advances this understanding in the nonmarket environment context, by illustrating that levels of control and justice, signalled by NMPv activities, also have a role to play in providing balance.

Applying CSR Posture Theory to Explain Approaches to Nonmarket Privacy

Castello and Lozano (2009) describe three approaches to CSR as 'CSR Postures', namely Risk Management CSR Posture, Integrated CSR Posture and Citizenship CSR Posture. Aligned to these CSR postures, Trapp (2012) proposes a three generational approach to CSR, namely First Generation CSR, Second Generation CSR and Third Generation CSR. Whilst approaches to NMPv in the Nonmarket Privacy Orientation Matrix are underpinned

by these three CSR Postures and Generations, a fourth approach emerges which expresses high justice-low control. This approach most likely evolved, in response to changing societal expectations emerging from the pervasive intrusions associated with the connected world (Johnson, 2019).

7.4.1.4 Devising New Outputs by Combining Theories

As the extant literature has largely neglected the nonmarket environment aspect of privacy, this research aimed to provide a gateway to deeper research into the relationship between privacy and nonmarket strategies such as CSR and CPA, and their influence on outcomes for the consumer. This research achieves this aim by reflecting on, and integrating, current approaches to privacy i.e., CIPO (Greenaway et al., 2015), together with current approaches to nonmarket strategy i.e., CSR Postures (Castello and Lozano, 2009). In doing so this research responds to a call from Luo et al. (2021) for further research in CPA, strategic CSR and SPI. By combining CIPO with CSR postures in this way, this research also conceptualises a framework of four approaches to NMPv, referred to as the Nonmarket Privacy Orientation Matrix and a series of NMPv activities characterising those NMPv orientations, referred to as the Nonmarket Privacy Activities Codebook. In this way, this research responds to a call from Greenaway et al. (2015) to construct a mechanism which can position a firm's approach to privacy, characterised by control and justice. These approaches, referred to in this research as NMPv orientations, and their associated NMPv activities, are summarised in Table 7.2.

Table 7.2 NMPv Activities Associated with NMPv Orientations

NMPv Orientation	NMPv Activities
Risk Management	• Information ownership. • Transaction focused on product for a price. • Inference-focused, aiming to profile for personalisation. • Privacy is aimed at internal stakeholders. • Privacy is driven by compliance. • No association between privacy and values. • Lobby for privacy beneficial for the organisation. • Low profile privacy management. • The organisation's privacy activities are aimed at stockholder/share value. • Limited budget is assigned to privacy activities. • An organisation's customers are not privacy aware. • The organisation has limited staff assigned to privacy activities.
Integrated	• Ownership is shared between customer and organisation where organisation benefits most. • Compliance is important but can be exceeded such as the provision of privacy training for employees beyond regulatory minimums. • The organisation is data-focused, aimed at extracting data from customer • Organisation's privacy activities aimed at external stakeholders. • Privacy associated with FIPPS and ethics codes. • Privacy is aimed at external stakeholders. • The organisation links privacy initiatives to the customer. • The organisation appoints a privacy representative(s) to middle management level.
Citizenship	• Information stewardship. • Compliance is the baseline, where the organisation aims is to exceed regulation. • Privacy is driven by values of ethics, trust, respect, loyalty. • The organisation's customers value privacy and monitor/manage their privacy initiatives. • Strategic collaboration with privacy advocacy groups. • The organisation appoints a privacy representative to the C-Suite. • The organisation associates privacy with their brand in corporate publications. • The organisation associates/funds privacy conferences.
Warrior	• Data fiduciary. • Compliance is important, but the social value of privacy is more important. Law can be breached to protect that value even at a cost to the organisation. • The organisation lobbies governments for privacy standards. more beneficial to customer/society than to organisation. • The organisation develops open standards for privacy.

7.4.2 Contribution to Practice

The preceding insights focus on theoretical contributions to this research, however the findings from this research yield important practical implications for practitioners and policymakers, which are discussed in this final section. The findings in this research highlight the importance of achieving the right mix of control and justice in a set of nonmarket privacy activities i.e., by doing 'privacy right' rather than just 'privacy rights'.

7.4.2.1 Implications for Organisations

Privacy assurance mechanisms play a fundamental role in lowering privacy concerns and building trust (e.g., Wu et al., 2012). Bansal et al. (2015) suggest that at present the universally accepted practice is to rely on the organisation's privacy-policies to convey the direct information about the user's control over their private data. This research suggests that CSR reports are additional mechanisms for privacy assurance that organisations need to consider. This research has practical significance for organisations, as it highlights the importance of CSR reports in alleviating privacy concerns, enhancing trust and increasing consumers' intentions to use a system or purchase a product/service. This research also confirms that an organisation's NMPv strategies, as communicated in their CSR reports, may signal varying levels of control or justice in protecting users' personal information.

Organisational approaches to privacy have typically been described in terms of their financial, ethical or legal responsibilities (Greenaway et al., 2015). However, this research highlights the need for privacy practitioners/corporate management to approach privacy beyond these responsibilities, to include wider societal concerns for privacy. Including these additional privacy responsibilities is important, as the nonmarket environment contributes to an organisation's bottom line and reputation (DenHond et al., 2014), and can enhance an organisation's competitive advantage (Lawton et al., 2013). However there is little guidance for privacy practitioners/corporate management as to how various NMPv

activities can influence responses in consumers and other important stakeholders. The results of this research enables practitioners to be better informed as to the potential return-on-investment for projects that involve activities exceeding privacy regulation. Using the Nonmarket Privacy Activities Codebook, practitioners can identify justice-based NMPv activities that are most likely to increase consumer trust and purchase intention/continuance intention, and most likely to reduce privacy concern, and then include these additional benefits when justifying their business case. However, how much justice-based NMPv activity should an organisation undertake? Whilst the Nonmarket Privacy Activities Codebook does not answer the 'how much' question, it does provide an organisation with the ability to determine and position its own NMPv orientation on the Nonmarket Privacy Orientation Matrix. The organisation is then better equipped to decide if that NMPv orientation is appropriate for their business.

Balancing Stakeholder Perspectives with Organisational Needs

Different nonmarket strategies send separate signals to stakeholders about an organisation's commitment to certain values, and the strength of those signals is decided by the position of stakeholders on those values (DenHond et al., 2014). For instance, CSR sends a signal to stakeholders about the firm's reliability and trustworthiness, where the strength of the signal depends on the intensity of the CSR activities and their effectiveness in achieving social goals (DenHond et al., 2014). In contrast, CPA sends a signal to stakeholders about the reliability of the firm, where the signal depends on whose interests the firm is pursuing in terms of its political goals and how well it executes its political strategy (DenHond et al., 2014). Therefore, practitioners and corporate leadership should carefully consider the impact that their NMPv activities have on stakeholders, and understand its key stakeholder's position on privacy. For instance, some stakeholders do not value their privacy highly (Athey et al., 2017), whereas others care deeply about their

privacy (Beke et al., 2018, Ghose, 2017, Wirtz and Lwin, 2009). Recent research on stakeholder cognition (Barnett et al., 2020; Barnett, 2014) may be helpful in this regard.

Aligning Nonmarket Privacy Strategies

Whilst highlighting the need to align NMPv strategies is newly introduced in this section, the need to align nonmarket strategies, such as CSR and CPA, is not new to the nonmarket literature. DenHond et al. (2014) refer to alignment and nonalignment of nonmarket strategies as 'playing on two chessboards' i.e., where an organisation's strategy for CSR differs to their CPA. They highlight the potential reputational effects of doing so. Where organisations align their CSR and CPA activities, they can more effectively resolve pressing social issues and can lead to constituencies revising their perception of the organisation as trustworthy or reliable (DenHond el., 2014). The researcher extends these effects, in the context of NMPv strategies, to also include the potential effects for privacy concern, consumer trust and purchase intention/continuance intention. In other words, where Corporate Social Privacy and Corporate Political Privacy are aligned, organisations are likely to experience increased consumer trust, increased purchase intention/continuance intention and reduced privacy concern.

7.4.2.2 Implications for Policymakers

Doing privacy rights versus doing privacy right reflects the debate between enabling versus mandatory regimes of governance. In this debate, Anand (2005) suggests that the free marketers argue that if enhanced governance practices were beneficial and desired by investors, firms competing for scarce capital would implement them voluntarily. Advocates, Anand (2005) suggest, would argue that an enabling regime is insufficient, since there is no guarantee that all firms will implement the reforms necessary to provide consumers with adequate privacy protections. Enabling regimes of privacy compliance are shaped by discretionary/voluntary frameworks such as FIPPs, where mandatory regimes

are shaped by regulatory frameworks such as GDPR (Kerry, 2018). Policymakers should be aware of and consider these jurisdictional challenges, particularly where they are underpinned by conflicting philosophies of governance.

Many current privacy regulations, such as the CCPA and the GDPR, take a risk-based approach, underpinned by privacy impact assessments that are focused on compliance and accountability (Hunton, 2014). In this way, organisations are mandated to take additional measures to protect data where risk demands it (Hunton, 2014). However, the ethical and social dimension of privacy is often absent in risk-based approaches to regulation (Mantelero,2018). This is because data protection legislation is largely focused on how organisations process personal data, rather than what organisations strategically do to extend or shape conditions for that processing. Policymakers should therefore consider privacy as a risk that extends beyond the direct processing of personal data and also consider an organisation's NMPv activities. Policymakers should also consider enhancing current privacy risk assessment frameworks, such as GDPR's Data Protection Impact Assessment (DPIA) framework, to consider not only the impact of privacy on consumers, but also the impact of privacy on society. Mantelero (2018) presents an excellent starting point for policymakers in this regard, by combining the Human Rights Ethical Impact Assessment (HREIA) framework with the GDPRs Data Protection Impact Assessment framework.

7.5 Limitations and Future Research

Despite the contributions this research makes to knowledge and practice, there are a number of limitations. The following section discusses seven key limitations, and concludes with additional recommendations for future research.

7.5.1 Limitations of the Dissertation

First, in selecting the Fortune 100 index to define the sample in Study One, the researcher accepts certain sample restrictions with respect to firm size and sector categorisation. For instance, the Fortune 100 index is limited to only the largest organisations in the US, and organisations such as Amazon are classified by Fortune as retail organisations rather than technology. Whilst there has been a tendency in the literature to investigate the CSR reports of only the largest firms, research in mid-sized organisations has largely been ignored (Morhardt, 2010). Future research could extend the sampling frame to include organisations of different sizes whose country of origin is subject to different data privacy regimes. Using a non-US sampling frame would also present an interesting avenue for future research. Lock and Seele (2017) highlight the uniqueness of the European market in this regard, as it combines regulated and unregulated national legislations in one market. Similarly, in order to control variance across the experimental conditions, survey participants in Study Two were limited to North American AMT workers. In this way, all participants in the survey may have relatively similar privacy expectations. For example, US participants would not have the expectation that their tax information would be published annually, as citizens in Sweden, Finland and Norway would do (Reuters, 2016). Future research could leverage non-US participants to explore and compare, consumer responses to NMPv across Europe, Asia, Africa etc.

The second limitation is generalisability. Critics of qualitative research often point to the issue of generalisability of contributions as a limitation of qualitative research (Conboy et

al., 2012), and indeed much has been written on this topic (e.g., Lee and Baskerville, 2012; Walsham, 1995). However, the goal of most qualitative studies is not to generalise but rather to provide a rich, contextualised understanding of a phenomenon through its intensive study (Pratt et al., 2020; Polit and Tatano-Beck, 2010). The application of the theory and concepts in this research are transferable to other future research settings. For example, the application of control and justice theories to position an organisation's approach to privacy, can similarly be applied in future research to position an organisation's approach to information security or to risk. Similarly, the method of using an Online Delphi Survey to determine levels of control and justice signalled by NMPv activities, can also be applied in future research to determine the levels of control and justice demonstrated by an organisation's reported cybersecurity activities.

Third, this research leveraged a series of measures for privacy awareness from Warner and Wang (2019), which are based on subjective self-assessment of knowledge. Such measures do not necessarily correspond with objective knowledge (Morrison, 2013). The literature however lacks objective privacy awareness measures (Correia and Compeau, 2017). Further research could determine an appropriate measure for 'actual' privacy awareness that not only includes current dimensions such as media awareness and previous privacy experience (Benamati et al., 2017), but also includes an objective assessment of a consumer's current understanding of organisational privacy responsibilities and data subject rights. The development of a set of objective measures for privacy awareness is important, and work by Correia and Compeau (2017) in this area, on the 'multidimensional situational model of information privacy awareness' would be a helpful starting point. Incorporating measures of an individual's privacy literacy would also be beneficial in this regard, i.e., their understanding of how information is used and how they can protect their information. Privacy literacy centres on the understanding of what may happen to personal information online, and the active protection of this information. In privacy literacy,

learners use the information they have about how their private information will be stored, used, or distributed, combined with their personal philosophy about what information should be public and private, to make informed decisions (Wissinger, 2017). The Online Privacy Literacy Scale (OPLIS) may present a good starting point (Trepte et al., 2015).

Fourth, it can often be difficult to determine whether an organisation is actually implementing the strategies reported in their corporate reports, or merely reporting to appease stakeholders (Kolk, 2003). Organisations can often overstate some of their privacy initiatives (Tate et al., 2010). Studies have referred to this practice as 'looking good rather than being good' (Chun et al., 2019). Thus, an interesting avenue for future research would be to conduct comparative research into what organisations 'say' in their CSR reports, versus what organisations 'do'. A good starting point for such research would be from Lock and Seele (2017) who found that CSR reports regulated by the 2014 EU directive on disclosure of non-financial information (European Commission, 2014) demonstrated increased credibility. Another issue with CSR reports is that CPA, a key nonmarket strategy, is often not reported in them. Future research could leverage multiple sources of information to include media reports, corporate annual reports and lobbying databases, in order to capture Corporate Political Privacy and Sociopolitical Privacy activities .

Fifth, levels of control and justice demonstrated by privacy activities is often fluid. For example, the appointment of a DPO was classified by the panel of SMEs as a justice-based activity. However, such an appointment is mandatory under certain GDPR conditions, and therefore this could also be interpreted as a control-based activity for any organisation obligated by GDPR to appoint a DPO. Different jurisdictions can often conduct philosophically different privacy regimes, based on either discretionary or mandatory governance frameworks. In this way a justice-based NMPv activity such as FIPPs can become a control-based NMPv activity in another jurisdiction e.g., GDPR, depending on the local regulatory requirements for an organisation or industry. The implication of this

limitation is that a global organisation could be positioned in the Integrated NMPv Orientation in one jurisdiction and in the Citizenship NMPv orientation in another. Further research could thus explore the application of the Nonmarket Privacy Orientation Matrix in different legal jurisdictions. In this way, a unified model of global nonmarket privacy orientations would be a valuable future model to develop. A good starting point for such a model would be Unified Theory of the Firm (Park and Shin, 2004).

Sixth, this research focuses on a consumer's intentions, as opposed to their actual behaviour. Whilst it is critical to understand the factors that influence the formation of intentions, those intentions do not always evolve into actual practice. Participants can also realise that their reported intention does not have any real and actual consequences (Bridoux et al., 2016). However, intentions are often used in studies of stakeholder's reactions (e.g., Sen et al., 2006), and are considered the most influential predictor of a consumer's actual behaviour (Ajzen, 1991). Intentions are often associated as responses to privacy concerns (Fortes and Rita, 2016), responses to trust (e.g., Kim et al., 2009, Kim et al., 2010, Liao et al., 2011) or responses to CSR (Mohr and Webb, 2005). Future research could apply analytic techniques, such as deep learning or machine learning, to further test our research framework and explore the ability of such a model to predict a consumer's actual responses. Future research could also explore additional responses such as spreading negative word of mouth (Son and Kim, 2008).

Seventh, in the research framework, consumer trust, privacy concern and purchase intention/continuance intention are modelled as dependent variables for three reasons. First, the exact relationship between these constructs remains a topic of debate (Miltgen and Peyrat-Guillard, 2014). For instance, trust is found to relate to both information privacy and disclosure (Fogel and Nehmad, 2009), and to mediate between them (e.g., Dinev and Hart, 2006), where privacy is found to be an antecedent to trust (e.g., Bélanger et al., 2002; Eastlick et al., 2006) or a consequence of trust (Malhotra et al., 2004; Bansal et

al., 2010). Second, the research is experimental, where the objective is on isolating causality. Finally, the aim of this research is to explore the influence of control and justice on these constructs rather than determining the whole range of interactions, antecedents, predictors, moderators, mediators etc. However, the researcher accepts the limitation of such an approach, and suggests that further research evaluate and explore the factors mediating and moderating the relationship between NMPv activities and these constructs.

7.5.2 Directions for Future Research

Whilst NMPv is clearly an under-researched topic, several additional fruitful avenues of future research emerge from this research. First, whilst this research focused on outcomes of NMPv activities for consumers, other stakeholders such as investors and employees, could be considered in future research. This research focused on private sector organisations, however public sector organisations such as healthcare and universities could also be investigated, particularly in the US where both have specific legislation protecting personal information e.g., the Health Insurance Portability and Accountability Act (HIPAA) for health, and the Family Educational Rights and Privacy Act (FERPA) for students.

Second, only sixty-five of the sample of Fortune 100 organisations produced CSR reports that referenced privacy. This research did not aim to explain or understand why organisations do not publish CSR reports or why they do not report privacy as part of their nonmarket activities. Allen and Peloza (2015) found that certain organisations, more specifically, Google and Facebook, benefitted from a brand halo that leads stakeholders to assume strong performance on CSR dimensions despite a CSR performance that is typically lower than competing organisations. Allen and Peloza (2015) suggest that if these organisations were to proactively communicate their CSR engagement to stakeholders, the brand halo would be tarnished, and the organisation's value would suffer. An interesting

avenue for future research would therefore be to determine from other sources, the NMPv activities of organisations who do not publish such reports. For instance, using media publications, press publications, and lobbying databases. These could then be used to position their approach to NMPv on the Nonmarket Privacy Orientation Matrix.

Third, this research did not aim to determine if an organisation's NMPv orientation leads them to conduct certain NMPv activities, or if an organisation's NMPv activities leads them to demonstrate certain NMPv orientations. For instance, 75% of organisations in the high-justice orientations of Citizenship and Warrior were involved in the US PRISM scandal of 2013, where the NSA and FBI used backdoors to these organisations to access personal customer information. Did the organisations 'choose' the Warrior and Citizenship orientation they demonstrate now, or did their orientation evolve from the activities conducted to repair the damage of the US PRISM scandal, or are there other nuances compelling them? This could be a fruitful avenue for future research, which could provide additional insight into how organisations behave in their nonmarket environment towards privacy.

Fourth, several organisational factors have been found to influence privacy concerns, for example, the completeness of a privacy policy (Andrade et al., 2002), website reputation (Andrade et al., 2002; Eastlick et al., 2006), and the comprehensiveness of a website (Pavlou et al., 2007). However, the influence of institutional factors affecting the nonmarket environment, such as reputation, credibility and legitimacy, have not been tested in the context of NMPv. Future research could determine if these institutional factors have an effect on a consumer's attitudes, behaviours or responses, in the context of NMPv. A good starting point for such research would be from Lock and Seele (2017) who develop a nonmarket activities credibility scale and apply it in the context of CSR reporting.

Fifth, both theoretical and anecdotal evidence suggests an important role of data sensitivity in information privacy (e.g., Margulis, 2003; Westin, 2003). Most respondents feel less

comfortable providing sensitive data such as medical records (Kam and Chismar, 2006). Lwin et al. (2007) found that sensitivity of information moderates the relationship between perceived company policy and privacy concerns. Future research could therefore measure consumer attitudes, responses and behaviours in the context of NMPv across differing situational contexts – in order to determine the moderating effect of sensitivity of information on the relationship between, for instance, perceived CSR and privacy concerns..

Sixth, several studies have found that nationality influences privacy concern (Dinev et al., 2006; Miltgen and Peyrat-Guillard, 2014), trust (Rosenbloom and Haefner, 2009) and purchase intention (Yunus and Rashid, 2016). As outlined previously, due to sample limitations, nationality is not tested in this research. Future research could therefore empirically examine the influence of nationality on the relationship between NMPv activities and outcomes for the consumer, for example, by comparing a sample of EU consumers and a sample of US consumers. Prior literature has also emphasised the relationship between people's culture and privacy (e.g., Milberg et al., 2000) with culture found to largely determine privacy concern (e.g., Bellman et al., 2004; Dinev et al., 2006) and any future investigations of nationality and NMPv could also consider accounting for cultural differences. Hofstede's (1991) framework of five cultural dimensions, used in previous privacy studies (e.g., Milberg et al., 2000; Bellman et al., 2004; Dinev et al., 2006; Posey et al., 2010) presents a good starting point for such research. Of particular interest in these cultural dimensions is 'power distance' (Hofstede, 2011). Power distance is defined as the extent to which less powerful members of organisations and institutions accept and expect unequal power distributions, not only from the perspective of the leaders, who hold power, but from the followers (Hofstede, 2011). In the context of the PRE Model of Privacy, 'power distance' can be used to reflect 'the extent to which consumers expect/accept the lack of control over their information, not only from the

perspective of the organisations who control their information but also from the perspective of the acceptance of other consumers.

Seventh, regardless of their nationality or culture, people's conceptualisations of privacy are dynamic over time (e.g., Boyd, 2007; Livingstone, 2008) and therefore age is an important factor to consider in privacy research. Whilst this research extends support for existing studies that find age influences privacy concern (Miltgen and Peyrat-Guillard, 2014) to the context of the nonmarket environment, future research could investigate the influence of age on the relationship between NMPv and consumer outcomes. Future research could also investigate the influence of age on privacy awareness or privacy literacy, and use actual rather self perceptions, as subjective assessments of knowledge do not necessarily correspond with objective knowledge (Morrison, 2013). This could be achieved by using a survey item composed of direct questions assessing the individuals understanding of their privacy rights under data protection legislation such as GDPR for Europeans survey participants, or HIPAA's privacy rule/CCPA for US participants etc.

Eighth, sixty percent of the CSR reports, investigated in Study One, reported their key stakeholders' position/concerns regarding the importance of privacy. For instance, in the materiality assessment sections of their CSR reports, Cisco, Microsoft, AT&T and Verizon reported that data privacy was a highly important issue/concern. Stakeholder responses to an organisation's NMPv activity can be shaped by whether the activity is expected to align with the personal values of consumers (Bhagwat et al., 2020). For instance, consumer responses to an organisation's SPI can be shaped by their comparison of the alignment of the organisation's values with their own – and thus influence their purchase decisions (Kim et al., 2018; Swaminathan et al., 2020). In other words, some individuals may consider that breaking the law is unacceptable under any circumstance. People want to trust people/ things where they see a fit with their values (van der Werff et al., 2019), therefore a good starting point for this would be to consider how value congruence shapes stakeholder trust

in the organisation (e.g., Schuh et al., 2018; van Dijk et al., 2019) in the context of privacy in the nonmarket environment.

Ninth, Culnan and Williams (2009) argue that organisations who exceed regulation experience less privacy breaches. Thus, organisations in high-justice NMPv orientations would be expected to experience less privacy incidents. However the researcher reviewed the reported data breaches of the organisations in the sample, as published in the Privacy Rights Clearinghouse (PRC) database, and could find no evidence to support that there were less breaches for organisations who exceeded privacy regulation. This could be because the PRC database is sourced from the state Attorneys General and the U.S. Department of Health and Human Services and is considered by PRC to be an incomplete look at the true scope of privacy breaches, in part due to varying state laws (Privacy Rights Clearinghouse, 2021). It could also be because not all privacy breaches need to be disclosed, or are concealed. This could be addressed in future research by including other sources of breach data, such as the Identity Theft Resource Centre and news/media reports.

Finally, privacy is often positioned at Chief Privacy Officer (CPO) level in industries such as finance and healthcare (IBM and Ponemon Institute, 2017). Whilst this research found that organisations in the tech industry and finance industry had reported the appointment of a CPO, few organisations in the healthcare and pharmaceutical industries reported the appointment of a CPO. Whilst scholars argue that the dynamic nature of privacy, and the formidable enforcement actions it informs, prompts organisations to appoint senior C-Suite level role(s) responsible for privacy (Bamberger and Mulligan, 2011), the motivations underpinning the appointment of such a role across industries, would also present an interesting avenue for future research.

7.6 Conclusion

This research set out to develop an understanding of the rather unexplored phenomenon of nonmarket privacy, to explore an organisation's approach to NMPv, and to examine the relationship between an organisation's NMPv activity and outcomes for the consumer, namely privacy concern, consumer trust, and purchase intention/continuance intention. Both the Nonmarket Privacy Orientation Matrix and the Nonmarket Privacy Activities Codebook represent a strong starting point for explaining and understanding a phenomenon previously underexplored in the literature. These frameworks can be retested and developed further in future research. The empirical findings highlight the importance of levels of control and justice in shaping those approaches, and outcomes for the consumer.

Despite the limitations outlined in this chapter, the research makes several valuable empirical and theoretical contributions to the privacy literature, the business and ethics literature, the IS literature and the nonmarket environment literature. These contributions include strong empirical support for the extension of a number of constructs to the nonmarket environment context, including privacy concern, consumer trust and purchase intention/continuance intention. The research extends control and justice theory, and PRE theory to provide a more comprehensive understanding of the influence of NMPv activities on consumer's privacy concern, consumer trust and purchase intention/continuance intention.

The research also provides actionable and practical insights for organisations and for policymakers on the implications of NMPv activities and strategies, which can help to address consumer's rising privacy concerns (PEW Research Centre, 2018) and their reducing consumer trust (Edelman, 2020). In doing so, organisations and governments may be encouraged to 'do privacy right rather than do privacy rights, as it benefits not just consumers, but organisations themselves.

REFERENCES

Ab Latif, R., Dahlan A., Mulud, Z., and Mat Nor, M. (2017). The Delphi technique as a method to obtain consensus in health care education research. *Education in Medicine Journal*, 9(3), pp. 89–102.

Aberson, C. (2019). *Applied Power Analysis for the Behavioral Sciences (2nd ed).* New York: Routledge.

Abdeen, A.; Rajah, E.; and Gaur, S. (2016). Consumers' beliefs about firm's CSR initiatives and their purchase behaviour. *Marketing Intelligence Planning*, 34(1), pp. 2–18.

Accenture and Ponemon Institute (2015). *How Global Organizations Approach the Challenge of Protecting Personal Data.* Available from: https://www.ponemon.org/local/upload/file/ATC_DPP%20report_FINAL.pdf. [Accessed July 2021].

United Nations Global Compact. (2005). *Towards responsible lobbying: Leadership and public policy. London, UK: AccountAbility*. Available from: https://d306pr3pise04h.cloudfront.net/docs/news_events%2F8.1%2Frl_final.pdf [Accessed July 2021].

Adams, J. (1965). Inequity in Social Exchange, IN L. Berkowitz (ed.), *Advances in Experimental Social Psychology*, Vol. 2 (Academic Press, New York), pp. 267– 299.

Aiman-Smith, L., Scullen, S., and Barr, S. (2002). Conducting Studies of Decision Making in Organizational Contexts: A Tutorial for Policy-Capturing and Other Regression-Based Techniques. *Organizational Research Methods,* 5(4), pp. 388-414.

Aguilera, R., Rupp, D., Williams, C., and Ganapathi, J. (2007). Putting the S back in corporate social responsibility: A multilevel theory of social change in organisations. *Academy of Management Review,* 32 (3), pp. 836-863.

Aguinis, H., and Bradley, K. (2014). Best Practice Recommendations for Designing and Implementing Experimental Vignette Methodology Studies. *Organizational Research Methods*, 17(4), pp. 351–371.

Aguinis, H., and Solarino, A. (2019). Transparency and replicability in qualitative research: The case of interviews with elite informants. *Strategic Management Journal,* 40(1), pp. 1291–1315.

Aguinis, H., Villamor, I., and Ramani, R. (2020). MTurk Research: Review and Recommendations. *Journal of Management,* 47(4), pp. 823-837.

Ajzen, I. (1991). The Theory of planned behaviour. *Organizational Behavior and Human Decision Processes,* 59(2), pp. 179–211.

Akins, R., Tolson, H.,and Cole, B. (2005). Stability of response characteristics of a Delphi panel: application of bootstrap data expansion. *BMC Medical Research Methodologies*, 5(37), pp. 1-12.

Akter, S., D'Ambra, J., and Ray, P. (2011). Trustworthiness in mHealth information services: An assessment of a hierarchical model with mediating and moderating effects using partial least squares (PLS). *Journal of the American Society for Information Science and Technology,* 62(1), pp.100-116.

Allard, N. (2008). Lobbying is an Honorable Profession: the Right to Petition and the Competition to be Right. Stanford Law And Policy Review*,* 19, pp. 23-68.

Allen, A., and Peloza, J. (2015). Someone to watch over me: The integration of privacy and corporate social responsibility. *Business Horizons*, 58, pp. 635-642.

Allstate (2019). 2019 CSR Report. https://www.allstatesustainability.com/content/documents/Allstate_2019SustainabilityReport.pdf. [Accessed July 2021]

Altman, I. (1975). *The environment and social behaviour: privacy, personal space, territory, crowding.* Monterey, CA: Brooks/Cole.

American Airlines (2019). 2019 CSR Report. https://s21.q4cdn.com/616071541/files/doc_downloads/crr/CRR-Report-2018.pdf. [Accessed July 2021]

American Express (2019). 2019 CSR Report. https://s1.q4cdn.com/692158879/files/doc_downloads/2020/American-Express-2019-2020-ESG-Report.pdf. [Accessed July 2021]

Amoroso, D., and Roman, F. (2015). Corporate social responsibility and purchase intention: The roles of loyalty, advocacy and quality of life in the Philippines. *International Journal of Management,* 4(1), pp. 25–41.

Anand, A. (2005). An Analysis of Enabling vs. Mandatory Corporate Governance Structures Post Sarbanes-Oxley. Delaware Journal of Corporate Law, 31(1), pp. 229-252.

Anastasiadis, S. (2014). Toward a View of Citizenship and Lobbying: Corporate Engagement in the Political Process. *Business and Society*, 53 (2). pp. 260-299.

Anastasiadis, S., Moon, J., and Humphreys, M. (2018). Lobbying and the responsible firm: agenda-setting for a freshly conceptualized field. *Business ethics: a European review*, 27 (3). pp. 207-221.

Anderson, C., and Agarwal, R. (2011). The digitization of healthcare: boundary risks, emotion, and consumer willingness to disclose personal health information. *Information Systems Research*, 22(3), pp. 469-490.

Anderson C., and Brion S. (2014). Perspectives on power in organizations. Annual Review of Organisational. Psychology. *Organisation Behavior.* 1, pp. 67–97.

Andrade, E., Kaltcheva, V., and Weitz, B. (2002). Self-Disclosure on the Web: The Impact of Privacy Policy, Reward, and Brand Reputation, IN: *Advances in Consumer Research,* S. Broniarczyk and K. Nakamoto (eds.). Valdosta, GA: Association for Consumer Research, pp. 350-353.

Anic, I., Budak, J., Rajh, E., Recher, V., Skare, V., and Skrinjaric, B. (2019). Extended model of online privacy concern: what drives consumers' decisions? O*nline Information Review*, 43(5), pp. 799-817.

Ansolabehere, S., Snyder, J., and Ueda, M. (2004). Did firms profit from soft money? *MIT Department of Economics Working Paper Series.*

Antwi, S., and Hamza, K. (2015) 'Qualitative and quantitative research paradigms in business research: A philosophical reflection'. *European Journal of Business and Management*, 7(3), pp. 217-225.

Apple (2019). Online CSR report. Available at www.apple.com/privacy/ and at www.apple.com/compliance/. [Accessed July 2021].

Arpaci, I. (2016). Understanding and predicting students' intention to use mobile cloud storage services. *Computers in Human Behavior,* 58(1), pp. 150-157.

Ashworth, L., and Free, C. (2006). Marketing Dataveillance and Digital Privacy: Using Theories of Justice to Understand Consumers Online privacy concerns. *Journal of Business Ethics,* 67 (2), pp. 107-123.

AT&T (2019). 2019 CSR Report. https://about.att.com/ecms/dam/csr/2019/library/corporate-responsibility/2019-2020-Summary.pdf. [Accessed July 2021].

Athey, S., Catalini, C., and Tucker, C. (2017). The digital privacy paradox: Small money, small costs, small talk. *National Bureau of Economic Research Working Paper,* No. 23488.

Atzmüller, C., and Steiner, P. (2010). Experimental vignette studies in survey research. *European Journal of Research Methods for the Behavioral and Social Sciences*, 6(3). pp. 128–138.

Aust, F., Diedenhofen, B., Ullrich, S., and Musch, J. (2013). Seriousness checks are useful to improve data validity in online research. *Behavior Research Methods*, 45(2), pp. 527–535.

Ba, S., and Pavlou, P. (2002). Evidence Of the Effect of Trust Building Technology in Electronic Markets: Price Premiums and Buyer Behavior. *MIS Quarterly*, 26(3), pp. 243-268.

Babbie, E. (2001). *Practice of Social Research.* Wadsworth Publishing Company , New York.

Bach, D, and Allen, D.(2010). What Every CEO Needs to Know About Nonmarket Strategy. *MIT Sloan Management Review,* 51(3), pp. 40-48.

Balakrishnan, J., Malhotra, A., and Falkenberg, L. (2017). Multi-Level Corporate Responsibility: A Comparison of Gandhi's Trusteeship with Stakeholder and Stewardship Frameworks. *Journal of Business Ethics,* 141, pp. 133-150.

Bamberger, K., and Mulligan, D. (2011). Privacy on the Books and on the Ground. *Stanford Law Review,* 63, UC Berkeley Public Law Research Paper No. 1568385, pp. 247-316.

Bandara, R., Fernando, M. and Akter, S. (2020). Managing consumer privacy concerns and defensive behaviours in the digital marketplace. *European Journal of Marketing*, 55(1), pp. 219-246.

Banerjee, B. (2008). 'Corporate social responsibility: the good, the bad and the ugly'. *Critical Sociology,* 34, pp. 51–79.

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

Bansal, G., Zahedi, F., and Gefen, D. (2008). The Moderating Influence of Privacy Concern on the Efficacy of Privacy Assurance Mechanisms for Building Trust: A Multiple-Context Investigation. Proceedings from Twenty Ninth International Conference on Information Systems *(*Paris).

Bansal, G., Zahedi, F., and Gefen, D. (2010). The Impact of Personal Dispositions on Information Sensitivity, Privacy Concern and Trust in disclosing health information online. *Decision Support Systems,* 49(2), pp. 138–150.

Bansal, G., Zahedi, F,. and Gefen, D. (2015). The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern. *European Journal of Information Systems*, 24 (6), pp. 624-644.

Bansal, G., Zahedi, F., and Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information and Management,* 53 (1), pp. 1-21.

Barends, A., and de Vries, R. (2019). Noncompliant responding: Comparing exclusion criteria in MTurk personality research to improve data quality. *Personality and Individual Differences*, 143(1), pp. 84-89.

Barnett, M. (2007). Stakeholder Influence Capacity and the Variability of Financial Returns to Corporate Social Responsibility. *Academy of Management Review*, 32 (3), pp. 794-816.

Barnett, M. (2014). Why Stakeholders Ignore Firm Misconduct: A Cognitive View. *Journal of Management*, 40(3), pp. 676-702.

Barnett, M., Henriques, I., and Husted, B. (2020). The Rise and Stall of Stakeholder Influence: How the Digital Age Limits Social Control. *Academy of Management Perspectives,* 34(1), pp. 48-64.

Baron, D. (1995). The Nonmarket Strategy System. *Sloan Management Review*, 37(1), pp. 73-85.

Baron, D. (2001). Private politics, corporate social responsibility and integrated strategy. *Journal of Economics and Management Strategy,* 10, pp. 7-45.

Baron, D. (2008). Siemens: The Anatomy of Bribery. *Stanford Graduate School of Business,* Case P68. 92(2), pp. 268-288.

Baron, J. (2012). Property as Control: The Case of Information, Telecommunications and Technology. *Law Review,* 18(2), pp. 367-418.

Baron, R., and Kenny, D. (1986). The Moderator-Mediator Variable Distinction in Social Psychological Research: Conceptual, Strategic, and Statistical Considerations. *Journal of Personality and Social Psychology,* 51(6), pp. 1173-1182.

Bauer, T. (2015). Responsible lobbying. *Journal of Corporate Citizenship*, 53(53), pp. 61–76.

Bauman, Z., and Lyon, D. (2013). *Liquid Surveillance: A conversation*. Polity Press. Cambridge.

Baysinger, B. (1984). Domain maintenance as an objective of business political activity: An expanded typology. *Academy of Management Review*, 9(1), pp. 248–258.

Baysinger, B., and Butler, H. (1985). Corporate Governance and the Board of Directors: Performance Effects of Changes in Board Composition. *Journal of Law, Economics, and Organization,* 1, pp. 101-124.

Beke, F., Eggers, F., and Verhoef, P. (2018). Consumer informational privacy: Current knowledge and research directions. *Foundations and Trends in Marketing*, 11(1), pp. 1-71.

Belanger, F. and Crossler, R. (2011). "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems". *MIS Quarterly*, 35(4), pp. 1017-1041.

Belanger, F., Hiller, J., and Smith, W. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. *Journal of Strategic Information Systems*, 11(3-4), pp. 245–270.

Bellman, S. Johnson, E., Kobrin, S., and Lohse, L (2004) International differences in information privacy concerns: a global survey of consumers. *The Information Society,* 20(5), pp. 313–324.

Benamati, J., Ozdemir, Z., and Smith, H. (2017). An empirical test of an Antecedents – Privacy Concerns – Outcomes model. *Journal of Information Science*, 43(5), pp. 583-600.

Best Buy (2019). 2019 CSR Report. https://corporate.bestbuy.com/wp-content/uploads/2019/06/FY19-full-report-FINAL-1.pdf. [Accessed July 2021].

Bhagwat, Y., Nooshin L., Warren, J., Beck, T., and Watson, G. (2020). Corporate Sociopolitical Activism and Firm Value. *Journal of Marketing*, 84(5), pp. 1-21.

Bhattacharya, C., and Elsbach, K. (2002). Us Versus Them: The Roles of Organizational Identification and Disidentification in Social Marketing Initiatives. *Journal of Public Policy and Marketing,* 21 (1), pp. 26–36.

Bhattacherjee, A. (2001). Individual Trust in Online Firms: Scale Development and Initial Testing. *Journal of Management Information Systems,* 19 (1), pp. 211-241.

Bhave, D., Teo, L., and Dalal, R. (2020). Privacy at work: A review and a research agenda for a contested terrain. *Journal of Management*, 46(1), pp. 127–164.

Bianchi, E.; Bruno, J.; and Sarabia-Sanchez, F. (2019). The impact of perceived CSR on corporate reputation and purchase intention. *European Journal Of Management Business and Economics,* 28 (5), pp. 206–221.

Bies, R. (1993). Privacy and Procedural Justice in Organizations. *Social Justice Research,* 6(1), pp. 69-86.

Bies, R., and Moag, J (1986). Interactional Justice: Communication Criteria of Fairness, IN: R. Lewicki, B. Sheppard and M. Bazerman (eds.), *Research on Negotiation in Organizations,* Vol. 1 (JAI Press, Greenwich, CT), pp. 43–55.

Bishop, F. (2015). Using mixed methods in health research: Benefits and Challenges. *British Journal of Health Psychology,* 20(2), pp. 1-4.

Blau, P. (1964). Justice in Social Exchange. *Sociological Inquiry,* 34 (2), pp. 193-206.

Blowfield, M., and Frynas, J. (2005). Setting New Agendas: Critical Perspectives on CSR in the Developing World. *International Affairs*, 81(1), pp. 499-513.

Blumentritt, T. (2003). Foreign Subsidiaries' Government Affairs Activities: The Influence of Managers and Resources. *Business and Society.* 42(2), pp. 202-233.

Boatright, J., and Peterson, J. (2003). Introduction: Special Issue on Finance. *Business Ethics Quarterly,* 13(3), pp. 265-270.

Bonate, P. (2000). *Analysis of Pretest-Posttest Designs*. CRC Press.

Bondy, K. (2008). The paradox of power in CSR: a case study on implementation. *Journal of Business Ethics*, 82(1), pp. 307–323.

Bonner, W., and Chiasson, M. (2005). If fair information principles are the answer, what was the question? An actor-network theory investigation of the modern constitution of privacy. *Information Organisation,* 15(1), pp. 267-293.

Boulkedid, R., Abdoul, H., Loustau, M., Sibony, O., Alberti, C. (2011). Using and reporting the Delphi method for selecting healthcare quality indicators: A systematic review. *PLOS One,* 6(6).

Boyatzis, R. (1998). *Transforming qualitative information: Thematic analysis and code development.* Thousand Oaks, CA: Sage.

Boyd, D. (2007) Why youth (heart) social network sites: the role of networked publics. IN *Youth, Identity and Digital Media* (D. Buckingham, Ed), MIT Press, Cambridge MA, pp.119–142.

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

Braun, V., and Clarke, V. (2013). *Successful qualitative research: A practical guide for beginners.* Sage. London.

Braun, V., and Clarke, V. (2020). One size fits all? What counts as quality practice in (reflexive) thematic analysis? *Qualitative Research in Psychology,* 18(3), 328-352.

Braun, V., and Clarke, V. (2021). Conceptual and design thinking for thematic analysis. *Qualitative Psychology.* Advance online publication.

Braun, V., Clarke, V., and Terry, G. (2014). Thematic analysis. In A. Lyons, and P. Rohleder (Eds.), *Qualitative Research in Clinical and Health Psychology*. Palgrave MacMillan.

Bridoux, F., Stofberg, N., and Den Hartog, D. (2016). Stakeholders' Responses to CSR Tradeoffs: When Other-Orientation and Trust Trump Material Self-Interest. *Frontiers in Psychology,* 6 (1992), pp. 1-18.

Brooks, J., McCluskey, S., Turley, E., and King., N. (2015). The Utility of Template Analysis in Qualitative Psychology Research. *Qualitative Research Psychology*, 12(2), pp. 202–222.

Brough, P., O'Driscoll, M., and Biggs, A. (2009). Parental leave and work-family balance among employed parents following childbirth: An exploratory investigation in Australia and New Zealand. *New Zealand Journal of the Social Sciences,* 4(1), pp. 71-87.

Bryman, A. (2012). *Social Research Methods, 4th edition*. Oxford, UK: Oxford University Press.

Brysbaert, M. (2019). How many participants do we have to include in properly powered experiments? A tutorial of power analysis with some simple guidelines. *Journal of Cognition,* 2(1), pp. 16.

Bucar, B., Glas, M., and Hisrich, R. (2003). Ethics and entrepreneurs: An international comparative study. *Journal of Business Venturing,* 18 (1), pp. 261-281.

Buchholz, R. (1992). *Business environments and public policy.* Englewood Cliffs, NJ: Prentice-Hall.

Buck A., Gross M., Hakim S., and Weinblatt J. (1993). Using the Delphi process to analyse social policy implementation: a post hoc case from vocational rehabilitation. *Policy Sciences,* 26(4), 271-288.

Buhrmester, M., Kwang, T., and Gosling, S. (2011). Amazon's Mechanical Turk: A New Source of Inexpensive, Yet High-Quality Data? *Perspectives on Psychological Science,* 6(1), pp. 3–5.

Butterworth, M. (2018). The ICO and artificial intelligence: The role of fairness in the GDPR framework. *Computer Law and Security Review*, 34(2), pp. 257-268.

Caldwell, C., Hayes, L., Bernal, P., and Karri, R. (2008). Ethical stewardship - Implications for leadership and trust. *Journal of Business Ethics*, 78, (1-2), pp. 153-164.

Caldwell C., Hayes, L., and Long, D. (2010). Leadership, Trustworthiness, and Ethical Stewardship *Journal of Business Ethics*, 96(4), pp. 497–512.

Caldwell, C., and Karri, R. (2005). Organizational Governance and Ethical Systems: A Covenantal Approach to Building Trust. *Journal of Business Ethics,* 58(1), pp. 249-259.

Callan, R. (2018). The Effects of Selection System Characteristics and Privacy Needs on Procedural Justice Perceptions: An Investigation of Social Networking Data in Employee Selection. *Doctor of Philosophy (PhD), Dissertation, Psychology,* Old Dominion University, DOI: 10.25777/3jfc-vz47.

Campbell, S., Cantrill, J., and Roberts, D. (2000). Prescribing indicators for UK general practice: Delphi consultation study. *Business and Marketing Journal*, 321, pp. 1-5.

Capron, L., and Chatain, O. (2008). Competitors' resource-oriented strategies: Acting on competitors' resources through interventions in factor markets and political markets. *The Academy of Management Review,* 33(1), pp. 97-121.

Carroll, A. (1979). A three dimensional conceptual model of corporate performance. *Academy of Management Review,* 4(4), pp. 497-505.

Carroll, A. (1991). The pyramid of corporate social responsibility: toward the moral management of organisational stakeholders. *Business Horizons*, 34(4), pp. 39-48.

Carroll, A. (2016). Carroll's pyramid of CSR: taking another look. *International Journal of Corporate Social Responsibility,* 1(3), pp. 1-8.

Carroll, A., and Buchholtz, A. (2003). *Business and Society: Ethics and Stakeholder Management (5th edn).* Thomson Publishing, South-Western Australia.

Castaldo, S., Perrini, F., Misani, N., and Tencati, A.(2009). The Missing Link Between CSR and consumer trust: The Case of Fair Trade Products. *Journal of Business Ethics*, 84, pp.1-15.

Castello, I., and Lozano, J. (2009). From risk management to citizenship corporate social responsibility: analysis of strategic drivers of change. *Corporate Governance,* 9(4), pp. 373-385.

Caudill E. and Murphy, P. (2000). Consumer Online Privacy: Legal and Ethical Issues. *Journal of Public Policy and Marketing*, 19(1), pp. 7-19.

Cavana, R., Sekaran, U., and Delahaye, B. (2001). *Applied Business Research: qualitative and quantitative methods.* Milton, QLD: John Wiley and Sons Australia.

Cavoukian, A. (2006). *Creation of a Global Privacy Standard.* Available at www.ipc.on.ca/images/Resources/gps.pd. [Accessed July 2021].

Cavoukian, A., Dix, A., and Emam, K. (2014). *The Unintended Consequences of Privacy Paternalism.* Information and Privacy Commisioner of Ontario, Canada.

Cavoukian, A. (2016). *Operationalizing privacy by design: A guide to implementing strong privacy practices*. Toronto, Canada: Office of the Privacy Commissioner, Ontario, Canada. Available at https://gpsbydesign.org/operationalizing-privacy-by-design-a-guide-to-implementing-strong-privacy-practices/. [Accessed July 2021].

Centrify and Ponemon Institute (2017). The impact of data breaches on reputation and share value. Available at https://www.centrify.com/media/4772757/ponemon_data_breach_impact_study_uk.pdf. [Accessed November 2021].

Chandler, D. (2016). *Strategic Corporate Social Responsibility*. Sage Publications.

Chandler, D. and Werther, W. (2013). *Strategic corporate social responsibility: stakeholders, globalization, and sustainable value creation (3rd ed.).* SAGE Publications.

Chang, K., Kim, I. and Li, Y. (2014). The Heterogeneous Impact of CSR Activities That Target Different Stakeholders. *Journal of Business Ethics*, 125, pp. 211–234.

Charlo, M., Ismael, and Muñoz, A. (2015). Sustainable Development and Corporate Financial Performance: A Study Based on the FTSE4GoodIBEX Index. *Business Strategy and the Environment,* 24(4), pp. 277-288.

Chatterji, A., and Toffel, M. (2018). The New CEO Activists. *Harvard Business Review*, 96 (1), pp. 78–89.

Chellappa, R., and Sin, R. (2005). Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma. *Information Technology and Management,* 6(2-3), pp. 181–202.

Chernev, A, and Blair, S. (2015). Doing Well by Doing Good: The Benevolent Halo of Corporate Social Responsibility. *Journal of Consumer Research*, 41(6), pp. 1412–1425.

Chia, R. (2003). Organization theory as a postmodern science. IN: H. Tsoukas and C. Knudsen (eds), *The Oxford Handbook of Organization Theory: Meta-Theoretical Perspectives*. Oxford: Oxford University Press, pp. 113-40.

Chieh-Peng, L., Shwu-Chuan, C., Chou-Kang, C., and Wan-Yu, L. (2011). Understanding Purchase intention During Product-Harm Crises: Moderating Effects of Perceived Corporate Ability and Corporate Social Responsibility. *Journal of Business Ethics,* 102, 455-471.

Chisholm, M. (2011). *Defining data ownership*. Available at: https://www.dataversity.net/defining-data-ownership/ [Accessed July 2021].

Choi, B., and La, S. (2013). The Impact of CSR(CSR) and Customer Trust on the Restoration of Loyalty after Service Failure and Recovery. *Journal of Services Marketing,* 27(3), pp. 223-233.

Christensen, D., Mikhail, M., Walther, B., and Wellman, L. (2017). From K Street to Wall Street: Political connections and stock recommendations. *The Accounting Review*, 92(3), pp. 87–112.

Chun, R., Argadona, A., Choirat, C. and Siegel, D. (2019). Corporate Reputation: Being Good and Looking Good. *Business and Society,* 58(6), pp. 1132-1142.

Cialdini, R., and Trost, M. (1998). *Social Influence: Social Norms, Conformity, and Compliance,* in The Handbook of Social Psychology, Volume II, Eds: D. Gilbert, S. Fiske, and G. Lindzey. New York: Oxford University, pp. 151-92.

Cigna (2019). 2019 CSR Report. https://www.cigna.com/static/www-cigna-com/docs/about-us/corporate-responsibility/report/cigna-connects-2019-corporate-responsibility-report.pdf. [Accessed July 2021].

Cisco (2019). CSR Report. https://www.cisco.com/c/dam/m/en_us/about/csr/csr-report/2019/_pdf/csr-report-2019.pdf. [Accessed July 2021].

Citi (2019). 2019 CSR Report Citi Group. https://www.citigroup.com/citi/about/esg/download/2019/Global-ESG-Report-2019.pdf. [Accessed July 2021].

Clarke, V., Braun, V., and Hayfield, N. (2015) Thematic Analysis. In: Smith, J.A., Ed., Qualitative Psychology: A Practical Guide to Research Methods, SAGE Publications, London, pp. 222-248.

Clawson, D., Neustadtl, A., and Weller, M. (1998). Dollars and Votes. Philadelphia, PA: Temple University Press.

Cohen, J. (1988). *Statistical power analysis for the behavioural sciences (2nd Ed).* Hillsdale, NJ: L Erlbaum Associates.

Collier, J., and Esteban, R. (2007). Corporate social responsibility and employee commitment. *Business Ethics*, 16 (1), pp. 19-33.

Collingridge, D. (2013). A primer on quantitized data analysis and permutation. *Journal of Mixed Methods Research*, 7(1), pp. 81–97.

Colquitt, J. (2001).On the Dimensionality of Organizational Justice: A Construct Validation of a Measure. *Journal of Applied Psychology*, 86 (3), pp. 386-400.

Colquitt, J., Piccolo, R., LePine, J., and Zapata, C. (2012). Explaining the Justice-Performance Relationship: Trust as Exchange Deepener or Trust as Uncertainty Reducer? *Journal of Applied Psychology*, 97(1), pp. 1-15.

Conboy, K., Fitzgerald, G. and Mathiassen, L. (2012). Qualitative Methods Research in Information Systems: Motivations, Themes, and Contributions. *European Journal of Information Systems,* 21(2), pp. 113-118.

Conger, S., Pratt, J. and Loch, K. (2013). Personal information privacy and emerging technologies. *Information Systems Journal*, 23(5), pp. 401–417.

Constas M. (1992). Qualitative analysis as a public event: the documentation of category development procedures. *American Educational Research Journal*. 29(2), pp. 253-266.

Correia, J., and Compeau, D. (2017). Information Privacy Awareness (IPA): A Review of the Use, Definition and Measurement of IPA. *Proceedings of the 50th Hawaii International Conference on System Sciences.*

Cote, C. (2021). What is a CSR report and why is it important? *Business Insights*, Harvard Business School Online. Available at https://online.hbs.edu/blog/post/what-is-a-csr-report. [Accessed September 2021].

Creswell, J. (1998). *Qualitative inquiry and research design: Choosing among five traditions*. Sage Publications, Inc.

Creswell, J. (2009). *Research Design: Qualitative, Quantitative, and Mixed Methods Approach, 3rd ed.* Thousand Oaks: Sage Publications.

Creswell, J., (2013*). Qualitative inquiry and research design: Choosing among five approaches, 3rd ed*. Thousand Oaks: Sage Publications.

Creswell, J. (2015) Revisiting mixed methods and advancing scientific practices. IN: Hesse-Biber, S, Johnson, RB (eds), *The Oxford Handbook of Multimethod and Mixed Methods Research Inquiry*, New York: Oxford University Press, pp. 61–71.

Creswell, J., and Plano Clark, V. (2007). *Designing and Conducting Mixed Methods Research.* Thousand Oaks, CA: Sage.

Creswell, J., and Plano Clark, V. (2011). *Designing and conducting mixed methods research (2nd ed.).* Thousand Oaks, CA: Sage.

Creswell, J., Plano Clark, V., Gutmann, M., and Hanson, W. (2003). Advanced mixed methods research designs. IN: A. Tashakkori, and C. Teddlie (Eds.), *Handbook of mixed methods in social and behavioural research*. Thousand Oaks, CA: Sage, pp. 209-240.

Creyer, E. (1997). The influence of firm behaviour on purchase intention: do consumers really care about business ethics. *The Journal of Consumer Marketing,* 14(6), pp. 421-432.

Cronbach, L. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika*, 16(3), pp. 297-334.

Cronk, J. (2018). *White Paper: Check or Mate? Strategic Privacy By Design*. International Association of Privacy Professionals (IAPP) Publications. Available at: https://iapp.org/resources/article/check-or-mate-strategic-privacy-by-design/. [Accessed August, 2021].

Crotty, M. (1998). *The foundations of social research: Meaning and perspective in the research process.* Thousand Oaks, CA: Sage.

Culnan, M., and Armstrong, P. (1999). "Information privacy concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation". *Organisational Science*, 10(1), pp. 104-115.

Culnan, M., and Bies, R. (2003). Consumer Privacy: Balancing Economic and Justice Considerations. *Journal of Social Issues*, 59(2), pp. 323-342.

Culnan, M., and Williams, C. (2009). How Ethics Can Enhance Organizational Privacy: Lessons from the ChoicePoint and TJX Data Breaches. *MIS Quarterly*, 33(4), pp. 673–687.

Currall, S., and Towler, A. (2003). Research methods in management and organisational research: toward integration of qualitative and quantitative techniques. IN: A. Tashakkori, and C. Teddlie (Eds), *Handbook of mixed methods in social and behavioural research.* Thousand Oaks, CA: Sage. pp. 513-526.

Cypress, B. (2017). Rigor, Reliability and Validity in Qualitative Research: Perspectives, Strategies, Re-Conceptualization and Recommendations. *Dimensions of Critical Care Nursing,* 36, pp. 253-263.

Daly, T., and Nataraajan, R. (2015). Swapping bricks for clicks: Crowdsourcing longitudinal data on Amazon Turk. *Journal of Business Research*, 68 (12), pp. 2603-2609.

Davis, J., Schoorman, F., and Donaldson, L. (1997). Davis, Schoorman, and Donaldson Reply: The Distinctiveness of Agency Theory and Stewardship Theory. *The Academy of Management Review,* 22(3), pp. 611-613.

Davis, K. (1960). Can Business Afford to Ignore Corporate Social Responsibilities?. *California Management Review, 2(1)*, pp. 70-76.

Davis, K., Frederick, W., and Blomstrom, R. (1980). *Business and Society, 2nd ed.*, McGraw-Hill, New York, NY.

Day, J., and Bobeva, M. (2005). A generic toolkit for the successful management of Delphi studies. *The Electronic Journal of Business Research Methodology,* 3(2), pp. 103-116.

DeCew, J. 2002. *Privacy*. Available from: http://plato.stanford.edu/entries/privacy/ [Accessed June 2021].

DenHond, F., Rehbein, K., Bakker, F., and Lankveld, H. (2014). Playing on two chessboards: Reputation effects between corporate social responsibility (CSR) and corporate political activity (CPA). *Journal of Management Studies*, 51(5), pp. 790-813.

Delbecq, A., de Ven, V., and Gustafson, D. (1975). *Group Techniques for Program Planning*, Scott, Foresman, Glenview, Illinois.

Dell (2019). 2019 CSR Report. https://corporate.delltechnologies.com/en-ie/social-impact/reporting/fy19-csr-report.htm. [Accessed July 2021].

Delta (2019). 2019 CSR Report. https://www.responsibilityreports.com/HostedData/ResponsibilityReports/PDF/NYSE_DAL_2019.pdf. [Accessed July 2021].

Denzin, N., and Lincoln, Y. (Eds) (2011). *The SAGE handbook of qualitative research.* Thousand Oaks, CA: Sage.

DeRoeck, K., and Delobbe, N. (2012), Do Environmental CSR Initiatives Serve Organizations' Legitimacy in the Oil Industry? Exploring Employees' Reactions Through Organizational Identification Theory, *Journal of Business Ethics*, 110(4), pp. 397-412.

Detomasi, D. (2008). The Political Roots of Corporate Social Responsibility. *Journal of Business Ethics,* 82(4), pp. 807-819.

DHS (2017). Department of Homeland Security's Privacy Incident Handling Guidance - Instruction Guide. Available at https://www.dhs.gov/sites/default/files/publications/047-01-008%20PIHG%20FINAL%2012-4-2017_0.pdf. [Accessed August 2021].

DHS. (2018). *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security.* Memorandum Number: 2008-01. US Dept of Homeland Security Privacy Office Publications. Available at: https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf. [Accessed July 2021].

Diefendorff, J., Greguras, G., and Fleenor, J. (2016). Perceived emotional demands abilities fit. *Applied Psychology*, 65(1), pp. 2–37.

Dinev, T. (2014). Why would we care about privacy? *European Journal of Information Systems*, 23(2), pp. 97–102.

Dinev, T., and Hart, P. (2004). Internet privacy concerns and their antecedents - measurement validity and a regression model. *Behavior and Information Technology*, 23(6), pp. 413-422.

Dinev, T., and Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, 17(1), pp. 61-80.

Dinev, T., Bellotto, M., Hart, P. Russo, V., and Serra, I. (2006). Internet Users' privacy concerns and Beliefs About Government Surveillance: An Exploratory Study of Differences Between Italy and the United States. *Journal of Global Information Management,* 14(4), pp. 1-37.

Dinev, T., Hart, P., and Mullen, M. (2008). Internet privacy concerns and beliefs about government surveillance–An empirical investigation. *The Journal of Strategic Information Systems*, 17(3), pp. 214–233.

Dinev, T., Xu, H., and Smith, H. (2009). Information Privacy Values, Beliefs and Attitudes: An Empirical Analysis of Web 2.0 Privacy, *Proceedings of 42th Hawaii International Conference on System Sciences, Hawaii.*

Disney (2019). 2019 CSR Report. https://thewaltdisneycompany.com/app/uploads/2020/02/CSR2019Report.pdf. [Accessed July 2021].

Dodd, M. (2015). Globalization, Pluralization, and Erosion: The Impact of Shifting Societal Expectations for Advocacy and Public Good. *The Journal of Public Interest Communications,* 2(2), pp. 1-17.

Dodd, M., and Supa, D. (2015). Testing the Viability of Corporate Social Advocacy as a Predictor of Purchase Intention. *Communication Research Reports,* 32 (4), pp. 287–293.

Doh, J., Lawton, T., and Rajwani, T. (2012). Advancing nonmarket strategy research: Institutional perspectives in a changing world. *Academy of Management Perspectives,* 26(3), pp. 22-39.

Donaldson L, and Davis J. (1991). Stewardship Theory or Agency Theory: CEO Governance and Shareholder Returns. *Australian Journal of Management*. 16(1), pp. 49-64.

Donaldson, T., and Dunfee, T. (1999). *Ties That Bind: A Social Contracts Approach to Business Ethics.* Harvard Business School Press. Boston. MA.

Donaldson, T. and Preston, L. (1995). The Stakeholder Theory of the Corporation: Concepts, Evidence and Implications. *The Academy of Management Review*, 20(1), pp. 65-69.

Dorfman, L., Cheyne, L., Friedman, A., and Gottlieb, M. (2012). Soda and Tobacco Industry CSR Campaigns: How Do They Compare? *PLoS Medicine*, 9(6), pp.1-7.

Doyle, L., Brady, A., and Byrne, G. (2009). An overview of mixed method research. *Journal of Research in Nursing*, 14 (2), pp.175-185.

Doyle, L., Brady, A., and Byrne, G. (2016). An overview of mixed method research - revisited. *Journal of Research in Nursing*, 21(8), pp.623-635.

Druckman, J., Green, D., Kuklinski, J., and Lupia, A. (2011). Experiments: An introduction to core concepts. IN: J. Druckman, D. Green, J. Kuklinski, and A. Lupia (Eds.), *Cambridge Handbook of Experimental Political Science,* Cambridge: Cambridge University Press, pp. 15–26.

Du, J., Bai, T., and Chen, S. (2019). Integrating corporate social and corporate political strategies: Performance implications and institutional contingencies in China. *Journal of Business Research*, 98 (1), pp. 299-316.

Du, S., Bhattacharya, C. and Sen, S. (2007). Reaping relational rewards from corporate social responsibility: the role of competitive positioning. *International Journal of Research in Marketing*, 24(3), pp. 224-241.

Du, S., Bhattacharya, C., and Sen, S. (2010). CSR and Competitive Advantage: Overcoming the Trust Barrier. *Management Science,* 57(9), pp.1528-1545.

Dwyer, C., Hiltz, S., and Passerini, K. (2007). Trust and privacy concern within social networking sites: A Comparison of Facebook and MySpace. Proceedings of the Thirteenth Americas Conference on Information Systems, Keystone, Colorado.

Eastlick, M., Lotz, S., and Warrington, P. (2006). Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. *Journal of Business Research,* 59(8), pp. 877–886.

Eddy, E., Stone, D., and Stone-Romero, E. (1999). The effects of information management policies on reactions to human resource information systems: An integration of privacy and procedural justice perspectives. *Personnel Psychology*, 52(1), pp. 335-358.

Edelman. (2018). *Brands Take a Stand*. Available at: https://www.edelman.com/news-awards/two-thirds-consumers-world. [Accessed July 2021].

Edelman. (2020). Edelman Trust Barometer 2020. Available at: https://www.edelman.com/trust/2020-trust-barometer. [Accessed July 2021].

Eisenhardt, K. (1989). Building theories from case study research. *Academy of Management Review,* 14(4), pp. 532–550.

Elkington, J. (1999). *Cannibals with forks : the triple bottom line of 21st century business*. Oxford: Capstone.

Emerson, R. (1976). Social exchange theory. *Annual Review of Sociology*, 2(1), pp. 335-362.

Erdfelder, P., Lang, A., and Buchner, A. (2007). G*Power 3: A flexible statistical power analysis program for the social, behavioural, and biomedical sciences. *Behavior Research Methods,* 39(2), pp. 175–191.

Etikan, I., Abubakar, S., Rukayya, M., and Alkassim, S. (2016). Comparison of Convenience Sampling and Purposive Sampling. *American Journal of Theoretical and Applied Statistics*, 5(1), pp. 1-4.

Ernst and Young (2018). *Nonfinancial disclosures are essential to most institutional investors*. Available from: https://www.ey.com/en_ae/news/2018/11/nonfinancial-disclosures-are-essential-to-most-institutional-investors. [Accessed July 2021].

European Commission (2014). The EU Directive on disclosure of non-financial information. Available at http://ec.europa.eu/internal_market/accounting/non-financial_reporting/index_en.htm). [Accessed September 2021].

Experian (2001). Best Buy Case Study: Data contributes to Best Buy's successful Customer Relationship Management (CRM) strategy. Available at https://www.experian.com/case_studies/best_buy.pdf. [Accessed November 2021].

Farooq, O., Payaud, M., and Merunka, D. (2013). The Impact of CSR on Organizational Commitment: Exploring Multiple Mediation Mechanisms. *Journal of Business Ethics*, 125(4), pp. 563-580.

Fed Ex (2019). 2019 CSR Report. https://www.fedex.com/content/dam/fedex/us-united-states/sustainability/gcrs/FedEx_GCR_FINAL_4.17.19_144dpi.pdf. [Accessed July 2021].

Feilzer, M. (2010). Doing mixed methods research pragmatically: Implications for the rediscovery of pragmatism as a research paradigm. *Journal of Mixed Methods Research,* 4(2), pp. 6-16.

Fereday, J., and Cochrane, E. (2006). Demonstrating Rigor Using Thematic Analysis: A Hybrid Approach of Inductive and Deductive Coding and Theme Development. *International Journal of Qualitative Methods,* 5(1), pp. 80-92.

Fessmann, J. (2016). The emerging field of public interest communications. In E. Oliviera, A. D. Melo, & G. Gonclaves (Eds.). *Strategic communication in non-profit organizations: Challenges and alternative approaches* (pp. 13-34). Wilmington, DE: Vernon.

Festinger, L. (1953). Laboratory Experiments. IN: *Research Methods in the Behavioral Sciences,* eds L. Festinger and D. Katz (New York, NY: Holt, Rinehart and Winston), pp. 136-172.

Fetters M., Curry L., and Creswell J. (2013). Achieving integration in mixed methods designs-principles and practices. *Health Service Research*, 48(6), pp. 2134-2156.

Fia, M., and Sacconi, L. (2019). Justice and Corporate Governance: New Insights from Rawlsian Social Contract and Sen's Capabilities Approach. *Journal of Business Ethics*, 160(4), pp. 937-960.

Fink, C. and Whelan, T. (2016). The Comprehensive Business Case for Sustainability. *Harvard Business Review*. Available at: https://hbr.org/2016/10/the-comprehensive-business-case-for-sustainability. Accessed [June, 2021].

Firestone, W. (1987). Meaning in Method: The Rhetoric of Quantitative and Qualitative Research. *Educational Researcher,* 16(7), pp. 16-21.

Fleetwood, S. (2005). Ontology in organisation and management studies: A critical realist perspective. *Organization,* 12(1), pp. 197–222.

Flyverbom, M., Deibert, R. and Matten, D. (2019). The Governance of Digital Technology, Big Data, and the Internet: New Roles and Responsibilities for Business. *Business and Society*, 58(1), pp. 3-19.

Fogel, J., and Nehmad, E. (2009). Internet social networking communities: Risk taking, trust and privacy concerns. *Computers in Human Behavior*, 25(2), pp. 153–160.

Fooks, G., Gilmore, A., Colin, J., Holden, A. and Lee, K. (2013). The Limits of Corporate Social Responsibility: Techniques of Neutralization, Stakeholder Management and Political CSR. *Journal of Business Ethics,* 112(2), pp. 283-299.

Forbes (2011). *So, What Are These Privacy Audits That Google And Facebook Have To Do For The Next 20 Years?*. Available at: https://www.forbes.com/sites/kashmirhill/2011/11/30/so-what-are-these-privacy-audits-that-google-and-facebook-have-to-do-for-the-next-20-years/?sh=459378415000. [Accessed July 2021].

Forbes (2020). *The Forbes List of Just Companies*. Available at https://www.forbes.com/just-companies/#6fab872c2bf0. [Accessed September 2021].

Ford (2020). 2020 CSR Report. https://media.ford.com/content/dam/fordmedia/North%20America/US/2020/06/24/Ford-Full-2020-Sustainability-Report.pdf. [Accessed July 2021]

Forrester (2018). *Embrace Privacy as Your Corporate Social Responsibilit*y. Available at https://www.forrester.com/blogs/embrace-privacy-as-your-corporate-social-responsibility-csr/. [Accessed August 2021].

Fortes, N., and Rita, P. (2016). privacy concerns and online purchasing behaviour: Towards an integrated model. *European Research on Management and Business Economics*, 22(3), pp. 167-176.

Fox, G., Clohessy, T., van der Werff, L., Rosati, P., and Lynn, T. (2021). Exploring the competing influences of privacy concerns and positive beliefs on citizen acceptance of contact tracing mobile applications. *Computers in Human Behavior,* 121(106806), 1-15.

Franklin K., and Hart (2006). Idea Generation and Exploration: Benefits and Limitations of the Policy Delphi Research Method. *Innovation Higher Education,* 31(1), pp. 237–246.

Frazier, M., Johnson, P., and Fainschmidt, S. (2013). Development and validation of a propensity to trust scale. *Journal of Trust Research*, 3(2), pp. 76-97.

Freeman, R. (1994). The politics of stakeholder theory: Some future directions. *Business Ethics Quarterly*, 4(4), pp. 409–421.

Freeman, R. (2001). A stakeholder theory of the modern corporation. *Perspectives in Business Ethics,* 3(1), pp. 144-154.

Freeman, R., Wicks, A., and Parmar, B. (2004). Stakeholder Theory and "The Corporate Objective Revisited". *Organization Science,* 15(3), pp. 364-369.

Fremeth, A., and Richter, B. (2011). Profiting from Environmental Regulatory Uncertainty: Integrated Strategies for Competitive Advantage. *California Management Review*, 54(1), pp. 145–165.

Fried, C. (1984). Philosophical Dimensions of Privacy. *American Philosophical Quarterly,* 21 (3), pp. 199 – 213.

Frynas, J., Child, J., and Tarba, S. (2017). Nonmarket social and political strategies – New integrative approaches and interdisciplinary borrowings. *British Journal of Management*, 52(4), pp. 1-23.

Frynas, J., and Stephens, S. (2015). Political corporate social responsibility: Reviewing theories and setting new agendas. *International Journal of Management Reviews,* 17(4), pp. 483-509.

Funk, R., and Hirschman, D. (2017). Beyond nonmarket strategy: Market actions as corporate political activity. Academy of Management Review, 42 (1), pp. 32-52.

Fang, Y., Chiu, C., and Wang, E. (2011). Understanding customers' satisfaction and repurchase intentions: An integration of IS success model, trust, and justice. *Internet Research,* 21(4), pp. 479-503.

Fuoli, M. (2018). Building a Trustworthy Corporate Identity: A Corpus-Based Analysis of Stance in Annual and CSR Reports. *Applied Linguistics*, 39(6), pp. 846-885.

Gaines-Ross, L. (2017). What CEOs Should Know About Speaking Up on Political Issues. *Harvard Business Review*. Available at: https://hbr.org/2017/02/what-ceos-should-know-about-speaking-up-on-political-issues.[Accessed July 2021].

Galbreath, J. (2010). How does corporate social responsibility benefit firms? Evidence from Australia. *European Business Review*, 22(4), pp. 411-431.

Gao, L., Aksel, K., and Xuesong, B (2015). Understanding consumers' continuance intention towards mobile purchase: A theoretical framework and empirical study – A case of China. *Computers in Human Behavior,* 53(2), pp. 249-262.

Gao, R., and Milanaik, R. (2020). Comparison of Survey Distribution through Amazon's Mechanical Turk and Traditional Single-Site Survey Distribution. *Pediatrics*, 146(1), pp.80-81.

Gao, Y. (2008). An ethical judgment framework for corporate political actions. *Journal of Public Affairs,* 8(3), pp. 153-163.

Garriga, E., and Melé, D. (2004). CSR Theories: Mapping the Territory. *Journal of Business Ethics,* 53(1-2), pp. 51–71.

Gartner (2020). *Gartner Predicts for the Future of Privacy 2020.* Available at: https://www.gartner.com/smarterwithgartner/gartner-predicts-for-the-future-of-privacy-2020/. [Accessed July 2021].

Gaudêncio, P., Coelho, A., and Ribeiro, N. (2017). The role of trust in corporate social responsibility and worker relationships. Journal of Management Development, 36(4), pp. 1-20.

Geertz, C. (1973). *Interpretation of Cultures.* New York: Basic Press.

Gefen, D., and Ridings, C. (2002). Implementation Team Responsiveness and User Evaluation of Customer Relationship Management: A Quasi-Experimental Study of Social Exchange Theory. *Journal of Management Information Systems,* 19(1), pp. 47-69.

General Motors (2019). 2019 CSR Report. https://www.gmsustainability.com/_pdf/resources-and-downloads/GM_2019_SR.pdf. [Accessed July 2021].

George, D., and Mallery, M. (2010). *SPSS for Windows Step by Step: A Simple Guide and Reference,* Boston: Pearson.

Gerlach, J, Eling, N, Wessels, N, and Buxmann, P. (2019). Flamingos on a slackline: Companies' challenges of balancing the competing demands of handling customer information and privacy. *Information Systems Journal*, 29(1), pp. 548–575.

Getz, K. (1993). Selecting corporate political tactics. IN: B. Mitnick (Ed.), *Corporate political agency:* Newbury Park, CA: Sage, pp. 152-170.

Ghose, A. (2017). Tap: Unlocking the mobile economy. MIT Press, Cambridge, MA

Giannarou, L., and Zervas, E. (2014). Using Delphi technique to build consensus in practice. *International Journal of Business Science and Applied Management*, 9(2), pp. 65-82.

Gibson, R., and Guthrie, J. (1996). The greening of public sector annual reports: Towards a benchmark, Readings in Accounting Developments in the Public Sector 1994-95, *Public Sector Accounting Centre for Excellence,* Australian Society of CPAs, Melbourne.

Gill, J., and Johnson, P. (2002). *Research Methods for Managers (3rd edn).* London, Sage.

Ginosar, A., and Ariel, Y. (2017). An analytical framework for online privacy research: what is missing? *Information and Management*, 54(7), pp. 948-957.

Glaveli, N. (2020). Corporate social responsibility toward stakeholders and customer loyalty: investigating the roles of trust and customer identification with the company. *Social Responsibility Journal.* (ahead-of-print).

Global Reporting Initiative (2016). *Defining What Matters in Materiality Assessments*. Available at: https://www.globalreporting.org/resourcelibrary/GRI-DefiningMateriality2016.pdf. [Accessed June 2021].

Global Reporting Initiative (2021). GRI 418, Customer Privacy Reporting Standards 2016. Available at https://www.globalreporting.org/how-to-use-the-gri-standards/gri-standards-english-language/. [Accessed November 2021].

Godfrey, P. (2005). The relationship between corporate philanthropy and shareholder wealth: a risk management perspective. *Academy of Management Review*, 30(4), pp. 777-798.

Goldberg, I., Hill, A., and Shostack, A. (2003). Trust, Ethics and Privacy. *Boston University Law Review, (81), pp. 101-116.*

Goldman Sachs (2019). 2019 CSR Report. https://www.goldmansachs.com/our-commitments/sustainability/sustainable-finance/documents/reports/2019-sustainability-report.pdf. [Accessed July 2021].

Gond, J., Igalens, J.,and Swaen, V. (2011). The Human Resources Contribution to Responsible Leadership: An Exploration of the CSR–HR Interface. *Journal of Business Ethics,* 98(1), pp. 115-132.

Goodman, C. (1987). The Delphi technique: a critique. *Journal of advanced nursing*, 12(6), pp. 729-734.

Google (2018). *Responsible AI Practices*. Available at: https://ai.google/responsibilities/responsible-ai-practices/?category=privacy. [Accessed June 2021].

Google (2019). Online CSR Report. https://sustainability.google/. [Accessed July 2021].

Goranova, M., and Verstegen Ryan, L. (2013). Shareholder Activism: A Multidisciplinary Review. *Journal of Management*, 40(5), pp. 1230–1268.

Governance and Accountability Institute (2020). 65% of the Russell 1000 Index published sustainability reports in 2019. Available at https://www.ga-institute.com/research/ga-research-collection/flash-reports/2020-russell-1000-flash-report.html. [Accessed September 2021].

Graeff, T., and Harmon, S. (2002). Collecting and using personal data: consumers' awareness and concerns. *Journal of Consumer Marketing*, 19 (4), pp. 302-318.

Grant, W. (2000). *Pressure groups and British politics.* Basingstoke, UK: Macmillan Press.

Gray, D., Royall, B., and Malson, H. (2017). Hypothetically speaking: Using vignettes as a stand-alone qualitative method. IN: V. Clarke, V. Braun, & D. Gray (Eds.), *Collecting Qualitative Data: A Practical Guide to Textual, Media and Virtual Techniques* UK: Cambridge University Press, pp. 45-70.

Greenaway, K, and Chan, Y. (2005). Theoretical explanations for firms information privacy behaviours. *Journal of the Association of Information Systems*, 6(6), pp. 171-198.

Greenaway, K., and Chan, Y. (2013). Designing a customer information privacy program aligned with organisational priorities. *MIS Quarterly Executive*, 12(3), pp. 137-150.

Greenaway, K., Chan, Y., and Crossler R. (2015). Company Information Privacy Orientation. A conceptual framework. *Information Systems Journal,* 25(6), pp. 579-606.

Greenberg, J. (1987). A Taxonomy of Organisational Justice Theories. *Academy of Management Review,* 12(1), pp. 9-22.

Greenberg, J. (1993). The Social Side of Fairness: Interpersonal and Informational Classes of Organizational Justice, IN: R. Cropanzano (eds.), *Justice in the Workplace: Approaching Fairness in Human Resource Management*. Lawrence Erlbaum Associates, Hillsdale, NJ, pp. 79–103.

Greenberg, J., and Folger, R. (1983). Procedural justice, participation, and the fair process effect in groups and organisations. IN: P. Paulus (Ed.), *Basic group processes.* New York : Springer-Verlag, pp. 235– 256.

Greenland, S., Senn, S., Rothman, K., Carlin, J., Poole, C., Goodman, S., and Altman, D. (2016). Statistical tests, P values, confidence intervals, and power: a guide to misinterpretations. *European Journal of Epidemiology,* 31(4), pp. 337–350.

Grimmer, M.; and Bingham, T. (2013). Company environmental performance and consumer purchase intentions. *Journal of Business Research*, 66(1), pp. 1945–1953.

Groenland, E. (2018). Employing the Matrix Method as a Tool for the Analysis of Qualitative Research Data in the Business Domain. *International Journal of Business and Globalisation,* 21(1), pp.119-134.

Guba, E. (1990). *The Paradigm Dialog*. Sage, California.

Guest, G. (2013). Describing mixed methods research: An alternative to typologies. *Journal of Mixed Methods Research,* 7(1), pp. 141–151.

Guest, G., MacQueen, K., and Namey, E. (2012). *Applied thematic analysis*. Thousand Oaks, CA: Sage.

Gwebu, K., Wang, J., and Wang, L. (2018). The Role of Corporate Reputation and Crisis Response Strategies in Data Breach Management. *Journal of Management Information Systems,* 35(2), pp. 683-714.

Hadani, M., and Coombes, S. (2015). Complementary relationships between corporate philanthropy and corporate political activity: An exploratory study of political marketplace contingencies. *Business & Society*, 54(6), pp. 859-881.

Hadani, M., Dahan N., and Doh J. (2015). The CEO as chief political officer: Managerial discretion and corporate political activity. *Journal of Business Research,* 68(11), pp. 2330-2337.

Hadani, M., Doh, J., Schneider, M. (2018). Corporate political activity and regulatory capture: How some companies blunt the knife of socially oriented investor activism. *Journal of Management,* 44(5), pp. 2064-2093.

Hadani, M., and Schuler, D.(2013). In search of El Dorado: The elusive financial returns on corporate political investments. *Strategic Management Journal*, 34(2), pp. 165-181.

Hair Jr, J., Hult, G., Ringle, C., and Sarstedt, M. (2017*). A primer on partial least squares structural equation modeling (PLS-SEM)* (2nd ed.). London, UK: Sage Publications.

Hajli, N., Sims, J., Zadeh, A., and Richard, M. (2017). A social commerce investigation of the role of trust in a social networking site on purchase intentions. *Journal of Business Research,* 71(1), pp. 133-141.

Hallebone, E., and Priest, J. (2009). *Business and Management Research: Paradigms and Practices.* Palgrave Macmillan.

Hambrick, D., and Wowak, A. (2021). CEO Sociopolitical Activism: A Stakeholder Alignment Model. *Academy of Management Review*, 46(1), pp. 33–59.

Hamilton, J., and Hoch, D. (1997). Ethical Standards for Business Lobbying: Some Practical Suggestions. *Business Ethics Quarterly*, 7(3), pp. 117 – 129.

Hanafin, S., and Brooks, A. (2007). Achieving consensus in developing a national set of child well-being indicators. Social Indicators Research, 80(1), pp. 79-104.

Hasselbalch, G., and Tranberg, P. (2016). *Data Ethics – The New Competitive Advantage*. Print A/S by Internet Society.

Hasson, F., Keeney, S., and McKenna, H. (2000). Research guidelines for the Delphi survey technique. *Journal of Advanced Nursing*, 32(4), pp. 1008-1015.

Hauser, D., Ellsworth, P., and Gonzalez R. (2018). Are Manipulation Checks Necessary? *Frontiers in Psychology,* 9(1), pp. 998-1009.

Hayes, A. (2018). *The PROCESS Macro*. Available at: https://www.processmacro.org/index.html. [Accessed July 2021].

Hayes A., and Rockwood, N. (2017). Regression-based statistical mediation and moderation analysis in clinical research: Observations, recommendations, and implementation. *Behaviour Research and Therapy,* 98(1), pp. 39-57.

Healy, M., and Perry, C. (2000). Comprehensive criteria to judge validity and reliability of qualitative research within the realism paradigm. *Qualitative Marketing Research: An International Journal,* 3(3), pp. 118–126.

Henle, C., Kohut, G., and Booth, R. (2009). Designing electronic use policies to enhance employee perceptions of fairness and to reduce cyberloafing: An empirical test of justice theory. *Computers in Human Behavior, 25*(4), pp. 902–910.

Hernandez, M. (2012). Toward an understanding of the psychology of stewardship. *Academy of Management Review*, 37(2), pp. 172-193.

Heron, J. and Reason, P. (1997). A participatory inquiry paradigm. *Qualitative Inquiry*, 3 (3), pp. 274-294.

Hersch, P., Netter, J., Pope, D. (2008). Do campaign contributions and lobbying expenditures by firms create "political" capital? *Atlantic Economic Journal*, 36, pp. 395-405.

Hess, J., (1995). Construction and assessment of a scale to measure consumer trust. *American Marketing Association,* 6, pp. 20-26.

Hill, K, and Fowles, J. (1975). The methodological worth of the Delphi forecasting technique, Technological *Forecasting and Social Change*, 7(2), pp. 179-192.

Hillman, A. and Hitt, M. (1999). Corporate political strategy formulation: A model of approach, participation, and strategy decisions. *Academy of Management Review*, 24(4), pp. 825-842.

Hillman, A., and Keim, G. (1995). International variation in the business-government interface: Institutional and organisational considerations. *Academy of Management Review,* 20(1), pp. 193–214.

Hillman, A., Keim, G., and Schuler, D. (2004). Corporate political activity: A review and research agenda. *Journal of Management*, 30(6), pp. 837-857.

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

Hoffman, D., Novak, T., and Peralta, M. (1999). Information privacy in the marketspace: Implications for the commercial uses of anonymity on the Web. *The Information Society,* 15(2), pp. 129–39.

Hofstede, G. (1991). *Cultures and organisations: Software of the mind.* New York: McGraw-Hill.

Hofstede, G. (2011). Dimensionalizing cultures: The Hofstede model in context. *Online Readings in Psychology and Culture, 2*nd Edition.

Holloway, I., and Todres, L. (2003). The status of method: Flexibility, consistency and coherence. *Qualitative Research,* 3(3), pp. 345–357.

Holtz, B. (2013). Trust primacy: a model of the reciprocal relations between trust and perceived justice. *Journal of Management*, 39(7), pp. 1891-1923.

Hong, I., and Cho, H. (2011). The impact of consumer trust on attitudinal loyalty and purchase intentions in B2C e-marketplaces: Intermediary trust vs. seller trust. *International Journal of Information Management,* 31(5), pp. 469-479.

Hong, W. and Thong, J. (2013). Internet privacy concerns: An Integrated Conceptualisation and four empirical studies. *MIS Quarterly,* 37(1), pp. 275–298.

Homans, G. (1961). *Social Behavior: Its Elementary Forms*. Routledge and Kegan Paul, London.

Homburg C, Stierl M, and Bornemann T. (2013). CSR in Business-to-Business Markets: How Organizational Customers Account for Supplier CSR Engagement. *Journal of Marketing*, 77(6), pp. 54-72.

Home Depot (2019). 2019 CSR Report. https://cloud.3dissue.net/17127/17182/17296/18142/index.html. [Accessed July 2021].

Hoofnagle, C., King, J., Li, S., and Turow, J. (2010). *How different are young adults from older adults when it comes to information privacy attitudes and policies?* Available from: https://repository.upenn.edu/asc_papers/399 [Accessed July 2021].

Hörisch, J., Freeman, R., and Schaltegger, S. (2014). Applying stakeholder theory in sustainability management. Links, similarities, dissimilarities, and conceptual framework. *Organization & Environment*, 27(4), pp. 328 –34.

Howe, C., and Nissenbaum, H. (2009). Resisting Surveillance in Websearch. IN: *Lessons From The Identity Trail: Anonymity, Privacy and Identify in a Networked Society,* edited by I. Kerr, V. Steves, and C. Lucock, NY: Oxford University Press, pp. 417-438.

Hoyt, C., Price, T., and Poatsy, L. (2013). The social role theory of unethical leadership. *The Leadership Quarterly*, 24 (2), pp. 712-723.

HP (2019). 2019 CSR Report. https://h20195.www2.hp.com/v2/GetDocument.aspx?docname=c06601778. [Accessed July 2021]

Hsu, C., and Sandford, B. (2007). The Delphi Technique: Making Sense of Consensus. *Practical Assessment, Research, and Evaluation*, 12(10), pp. 1-8.

Hu, B., Liu, J. and Zhang, X. (2020). The impact of employees' perceived CSR on customer orientation: an integrated perspective of generalized exchange and social identity theory. *International Journal of Contemporary Hospitality Management*, 32(7), pp. 2345-2364.

Hughes, K. (2012). A Behavioural Understanding of Privacy and its Implications for Privacy Law. *The Modern Law Review*, 75(5), pp. 806–836.

Hughes, R., and Huby, M. (2002). The application of vignettes in social and nursing research. *Journal of Advanced Nursing*, 37, pp. 382–386.

Hui, L., Teo, H, and Lee, S. (2007). The value of privacy assurance: an exploratory field experiment. *MIS Quarterly*, 31(1), pp. 19-33.

Hung, M., Yang, S., and Hsieh, T. (2012). An examination of the determinants of mobile shopping continuance. *International Journal of Electronic Business Management*, 10(1). pp. 29-37.

Hunton, A. (2014). *A Risk-based Approach to Privacy: Improving Effectiveness in Practice.* The Centre For Information Policy Leadership, Information Security and Online Privacy. Available from: https://www.huntonak.com/files/upload/Post-Paris_Risk_Paper_June_2014.pdf. [Accessed July, 2021].

Hydock, C. (2018). Assessing and overcoming participant dishonesty in online data collection. *Behavior Research Methods*, 50(2), pp. 1563-1567.

IBM (2019). 2019 CSR Report. https://ibmorg-public.s3.us-east.cloud-object-storage.appdomain.cloud/responsibility/reports-and-policies/Corporate%20Responsibility/IBM-2019-CRR(1).pdf?_ga=2.143123442.610250911.1635803133-1890788587.1635803133. [Accessed July 2021].

IBM and Ponemon Institute (2017). *Cost of a Data Breach Report 2017*. Available at: https://www.ponemon.org/research/ponemon-library/security/2017-cost-of-data-breach-study-united-states.html. [Accessed June 2021].

IBM and Ponemon Institute (2020). *Cost of a Data Breach Report 2020*. Available from: https://www.ibm.com/security/data-breach. [Accessed July 2021].

Identity Theft Resource Center (2020). The ITRC 2020 Data Breach Report. Available at https://notified.idtheftcenter.org/s/2020-data-breach-report. [Accessed November 2021].

Iglesias, O., Markovic, S., Bagherzadeh, M., and Singh, J. (2020). Co-creation: A key link between corporate social responsibility, customer trust, and customer loyalty. *Journal of Business Ethics*, 163(1), pp. 151-166.

Imai, K. (2017). *Quantitative Social Science: An Introduction*. Princeton University Press.

Ingram Micro (2018). 2018 CSR Report. https://usa.ingrammicro.com/media/Documents/ingrammicro/c/corpcomm/2018-CSR-Report.pdf. [Accessed August 2021].

Ingram Micro (2021). Company Overview. Available at https://corp.ingrammicro.com/en-us/company/overview. [Accessed November 2021].

International Standards Organisation (2021). ISO 26000 Standard for Social Responsibility. Available at https://www.iso.org/iso-26000-social-responsibility.html. [Accessed November 2021].

Introna, L. (2000). Workplace surveillance, privacy and distributive justice. *Academy of Management, SIGCAS Computers and Society,* 30(4), pp. 33-39.

Iqbal, S., and Pipon-Young, L. (2009). Methods - The Delphi method. *Psychologist,* 22(7), pp. 598-600.

Irish Times (2019). "Amazon faces investor pressure over facial recognition: SEC refuses to allow tech giant block motions from AGM agenda" Available at https://www.irishtimes.com/business/technology/amazon-faces-investor-pressure-over-facial-recognition-1.3900466. [Accessed November 2021].

Irish Times (2020). Tusla becomes first organisation fined for GDPR rule breach. Available at https://www.irishtimes.com/news/crime-and-law/tusla-becomes-first-organisation-fined-for-gdpr-rule-breach-1.4255692. [Accessed November 2021].

Ivankova, N., Creswell, J., and Stick, S. (2006). Using mixed methods sequential explanatory design: From Theory to Practice. *Field Methods*, 18(1), pp. 3-20.

Iyengar, S. (2011). Laboratory experiments in political science. IN: J. Druckman, D. Green, J. Kuklinski, & A. Lupia (Eds.), *Cambridge Handbook of Experimental Political Science,* Cambridge: Cambridge University Press, pp. 73–88.

Jacobs, J. (1996). Essential assessment criteria for physical education teacher education programs: A Delphi study. *Doctoral dissertation*, West Virginia University, Morgantown.

Jamali (2008). A Stakeholder Approach to Corporate Social Responsibility: A Fresh Perspective into Theory and Practice. *Journal of Business Ethics*, 82(1), pp. 213-231.

James, W., and Gunn, G. (2000). *Pragmatism and other essays*. New York: Penguin Books.

Janakiraman, R., Lim, J., and Rishika, R. (2018). The Effect of a Data Breach Announcement on Customer Behavior: Evidence from a Multichannel Retailer. *Journal of Marketing,* 82 (2), pp. 85-105.

Jensen, C., Potts, C. and Jensen, C. (2005). Privacy practices of internet users: Self-reports versus observed behaviour. *International Journal of Human-Computer Studies*, 63 (1), pp. 203-227.

Johnson, B., Connolly, E., and Carter, T. (2011). Corporate social responsibility: the role of Fortune 100 companies in domestic and international natural disasters. *Corporate Social responsibility and Environmental Management,* 18(6), pp. 352-369.

Johnson, B. and Turner, L. (2003). Data Collection Strategies in Mixed Methods Research. IN: Tashakkori, A. and Teddlie, C. (eds.) *Handbook of Mixed Methods in Social & Behavioral Research,* Thousand Oaks, CA: Sage Publications, pp. 297–319.

Johnson, D. (2009). *Computer Ethics*, 3rd ed. Pearson Education, Inc., Upper Saddle River, NJ.

Johnson, G. (2019). Privacy and the Internet of Things: Why Changing Expectations Demand Heightened Standards, Washington. University. Jurisprudence Review, 11 (2), pp. 345-374.

Johnson, J. (2016). The Value—and Limits—of Distributive Justice in a justice-centred approach to Information Privacy. *Proceedings of Digital Sociology Conference, at the Western Political Science Association 2016 Annual Meeting*.

Johnson, P. and Clark, M. (2006) Editors' introduction: Mapping the terrain: An overview of business and management research methodologies. IN: P. Johnson and M. Clark (eds.) *Business and Management Research Methodologies*, Sage, London, pp. xxv – lv.

Johnson, R., and Christensen, L. (2017). *Educational research: Quantitative, qualitative, and mixed approaches.* 6th ed. Los Angeles: Sage.

Johnson, R., and Onwuegbuzie, A. (2004). Mixed methods research: A research paradigm whose time has come. *Educational Researcher*, 33(7), pp. 14–26.

Johnson, R., Onwuegbuzie, A., and Turner, L. (2007). Toward a definition of mixed methods research. *Journal of Mixed Methods Research*, 1(2), pp. 112-133.

Jones, T. (1995). Instrumental Stakeholder Theory: A synthesis of ethics and economics. *Academy of Management Review*, 20(20), pp. 404-437.

Joppe, M. (2000). *The Research Process*. Available at: https://www.uoguelph.ca/hftm/research-process. https://www.uoguelph.ca/hftm/research-process. [Accessed July 2021].

Kam, L., and Chismar, W. (2006). Online self-disclosure: model for the use of internet-based technologies in collecting sensitive health information. *International Journal of Healthcare Technology and Management*, 7(3-4), pp. 218-132.

Kampen, J., and Swyngedouw, M. (2000). The Ordinal Controversy Revisited. *Quality and Quantity*, 34, pp. 87-102.

Karns, G. (2011). Stewardship: A new vision for the purpose of business. *Corporate Governance.* 11(4), pp. 337-347.

Keeney, S., Hasson, F., and McKenna, H. (2007). Consulting the oracle: Ten lessons from using the Delphi technique in nursing research. *Methodological Issues in Nursing Research*, 53(2), pp. 205-212.

Keeney, S. Hasson, F., and Mckenna, H. (2011). The Delphi Technique in Nursing and Health Research. Wiley-Blackwell.

Kelley, H., and Thibaut, J. (1978). *Interpersonal Relations A Theory of Interdependence*. New York: John Wiley and Sons.

Kelly, L., and Cordeiro, M. (2020). Three principles of pragmatism for research on organizational processes. Methodological Innovations, 13(2), pp. 1-10.

Kenton, W. (2021). *The Fortune 100*. Available at: https://www.investopedia.com/terms/f/fortune-100.asp. [Accessed July 2021].

Kerlinger F. (1973). *Foundations of behavioural research*. New York: Holt, Rinehart, and Winston, Inc.

Kerr, W., Lincoln, W., and Mishra, P. (2011). The Dynamics of Firm Lobbying. *American Economic Journal: Economic Policy,* 6(4), pp. 343-379.

Kerry, C. (2018). *Why protecting privacy is a losing game today—and how to change the game.* The Brookings Institute. Available at https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/ [Accessed November 2021].

Keppel, G. (1991). *Design and analysis: A researcher's handbook (3rd ed.).* Englewood Cliffs: Prentice-Hall, Inc.

Kim H., and Huh, J. (2017). Perceived Relevance and Privacy Concern Regarding Online Behavioral Advertising (OBA) and Their Role in Consumer Responses. *Journal of Current Issues and Research in Advertising,* 38(1), pp.92-105.

Kim, D., Ferrin, D,. and Rao, H. (2008). 'A trust-based consumer decision-making model in electronic commerce: the role of trust, risk, and their antecedents'. *Decision Support Systems*, 44 (2), pp. 554–564.

Kim, D., Ferrin, D., and Rao, H. (2009). Trust and satisfaction, two stepping stones for successful e-commerce relationships: a longitudinal exploration. *Information Systems,* 20 (2), pp. 237–257.

Kim, J., Kim, W., and Park, S. (2010). Consumer perceptions on web advertisements and motivation factors to purchase in the online shopping. *Computers in Human Behavior*, 26(5), pp. 1208–1222.

Kim, J. (2008). Corporate lobbying revisited. *Business and Politics*, 10(2), pp. 1-23.

Kim, J., Park, B., and DuBois, D. (2018). How Consumers' Political Ideology and Status-Maintenance Goals Interact to Shape Their Desire for Luxury Goods. *Journal of Marketing*, 82(6), pp. 132–149.

Kim, S. (2019). The process model of corporate social responsibility (CSR) communication: CSR communication and its relationship with consumers' CSR knowledge, trust, and corporate reputation perception. *Journal of Business Ethics*, 154(1), pp. 1143–1159.

Kim, Y., and Cribbie, R. (2018). ANOVA and the variance homogeneity assumption: Exploring a better gatekeeper. *British Journal of Mathematical and Statistical Psychology*, 71(1), pp.1-12.

Kim, S., Milliman, J., and Lucas, A. (2021). Effects of CSR on affective organizational commitment via organizational justice and organization-based self-esteem. International Journal of Hospitality Management, 92,102691.

King, A., and. Lenox, M. (2000). Industry Self-Regulation without Sanctions: The Chemical Industry's Responsible Care Program. *Academy of Management Journal*, 43(4), pp. 698–716.

King, N. (2004). Using templates in the thematic analysis of text. IN: Cassell, C., Symon, G. (Eds.), *Essential guide to qualitative methods in organisational research*. London, UK: Sage, pp. 257–270.

King, N., and Horrocks, C. (2010). *Interviews in qualitative research,* Sage, London.

KPMG (2013). *The KPMG Survey of Corporate Responsibility Reporting*. Available at : https://assets.kpmg/content/dam/kpmg/pdf/2013/12/corporate-responsibility-reporting-survey-2013.pdf. [Accessed July 2021].

Kolk A. (2003). Trends in Sustainability Reporting by the Fortune Global 250. *Business Strategy and the Environment,* 12(5), pp. 279–291.

Kolm, S. (1997). *Modern Theories of Justice*. MIT Press, Cambridge.

Korschun, D., Rafieian, H., Aggarwal, A., and Swain, S. (2016). Taking a Stand: Consumer Responses When Companies Get (or Don't Get) Political. *SSRN Electronic Journal*. dx.doi.org/10.2139/ssrn.2806476.

Kotler, P., and Sarkar, C. (2017). Finally, Brand Activism!. *The Marketing Journal*, Available at: http://www.marketingjournal.org/finally-brand-activism-philip-kotlerand-christian-sarkar/. [Accessed July 2021].

Krishen, A., Raschke, R., Close S, and Pushkin, R. (2017). A power-responsibility equilibrium framework for fairness: Understanding consumers' implicit privacy concerns for location-based services. *Journal of Business Research,* 73(10), pp. 1016-1027.

Kroger (2020). 2020 CSR Report. https://www.thekrogerco.com/wp-content/uploads/2021/07/Kroger-2020-ESG-Report.pdf. [Accessed July 2021].

Kroszner, R. and Stratmann, T. (2005). Regulation and Deregulation of the U.S. Banking Industry: Causes, Consequences, and Implications for the Future. IN: N. Rose (ed) *Economic Regulation and Its Reform: What Have We*. University of Chicago Press, pp. 485-543.

Kucuk, S. (2016). Exploring the legality of consumer anti-branding activities in the digital age. *Journal of Business Ethics*, 139(1), pp. 77– 93.

Kuckartz, U. (2014). *Qualitative text analysis: A guide to methods, practice & using software*. Los Angeles, CA: Sage.

Kuckartz, U., and Rädiker, S. (2019). *Analyzing qualitative data with MAXQDA. Text, audio, and video.* Cham: Springer Nature.

Kumar, S., Kumar, P., and Bhasker, B. (2018) Interplay between trust, information privacy concerns and behavioural intention of users on online social networks. *Behaviour and Information Technology*, 37(6), pp. 622-633.

Kuokkanen, H., and Sun, W. (2020). Companies, Meet Ethical Consumers: Strategic CSR Management to Impact Consumer Choice. *Journal of Business Ethics*, 166, pp. 403–423.

Kuusi, O. (1999). Expertise in the future use of generic technologies. Epistemic and methodological considerations concerning Delphi Studies. *VATT Research Report No. 59, Helsinki Government Institute for Economic Research.*

Laczniak, G. and Murphy, P. (1993). *Ethical Marketing Decisions: The Higher Road*. Allyn & Bacon, Boston.

Lance, C., Butts, M., and Michels, L. (2006). The Sources of Four Commonly Reported Cut-off Criteria: What Did They Really Say? *Organizational Research Methods*, 9(2), pp. 202-213.

Lantos, G. (2001). The boundaries of strategic corporate social responsibility. *Journal of Consumer Marketing*, 18(7), pp. 595–632.

LaPlume, A., Sonpar, K., and Lutz, R. (2008). Stakeholder theory: Reviewing a theory that moves us. *Journal of Management*, 34(6), pp. 1152–1189.

Lascelles, D. (2005). *The ethics of influence: Political donations and lobbying.* London: Institute of Business Ethics.

Latapi-Agudelo, M., Johannsdottir, L. and Davidsdottir, B. (2019). A literature review of the history and evolution of corporate social responsibility. *International Journal of Corporate Social Responsibility,* 4(1), pp. 1-23.

Laube, S., and Böhme, R. (2016). The economics of mandatory security breach reporting to authorities. *Journal of Cybersecurity*, 2(1), pp. 29 – 41.

Laudon, K. (1996). Markets and Privacy. *Communications of the ACM,* 39(9), pp. 92-104.

Lauer, T., and Deng, X. (2007). Building online trust through privacy practices, International *Journal of Information Security*, 6(5), pp. 323-331.

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

Lawton, T., McGuire, S., and Rajwani, T. (2013). CPA: A Literature Review and Research Agenda. *International Journal of Management Reviews,*15(1), pp. 86-105.

Lawton, T., and Rajwani, T. (2015). (eds) *The Routledge Companion to Non-Market Strategy.* Routledge UK .

Lawton, T., Doh, J., and Rajwani, T. (2014). *Aligning for advantage.* Oxford, England: Oxford University Press.

Lazaro, C., and Le Metayer, D. (2015). Control over personal data: true remedy or fairy tale?'. *SCRIPTed*, 12(1), pp. 3-29.

Lee, A. (1991) Integrating Positivist and Interpretive Approaches to Organizational Research. *Organization Science*, 2(4), pp. 342-365.

Lee, A., and Baskerville, R. (2012). Conceptualizing Generalizability: New Contributions and a Reply. MIS Quarterly, 36 (3), pp. 749-761.

Lee, D., Moon, J., and Kim, Y. (2015). Antecedents and consequences of mobile phone usability: Linking simplicity and interactivity to satisfaction, trust, and brand loyalty. *Information and Management*, 52(3), pp. 295-304.

Lee, H., Park, T., Moon, H., Yang, Y., and Kim, C. (2009). Corporate philanthropy, attitude towards corporations, and purchase intentions: A South Korea study. *Journal of Business Research*, 62(10), pp. 939-946.

Lee, H., Wong, S., Oh, J., and Chang, Y. (2019). Information privacy concerns and demographic characteristics: Data from a Korean media panel survey. *Government Information Quarterly*, 36(2), pp. 294-303.

Lee, M., and Turban, E. (2001). A trust model for consumer internet shopping. International *Journal of International Commerce*, 6(1), pp. 75-91.

Leech, N., Barrettt, K., and Morgan, G. (2005). *SPSS for Intermediate Statistics: Use and Interpretation.* Psychology Press.

Leech, N., Barrettt, K., and Morgan, G. (2015). *SPSS for Intermediate Statistics: Use and Interpretation, 5th ED.* Routledge.

Leininger, M. (1992). Current issues, problems, and trends to advance qualitative paradigmatic research methods for the future. *Qualitative Health Research*, 2, pp. 392–415.

Lessig, L. (2002). Privacy as Property. *Social Research*, 69(1), pp. 247-269.

Leventhal, G. (1980). What should be done with equity theory? New approaches to the study of fairness in social relationships. IN: K. Gergen, M. Greenberg, and R. Willis (Eds.), *Social exchange: New advances in theory and research*,, New York : Plenum Press, pp. 27– 55.

Li, Y. (2011). Empirical Studies on Online Information privacy concerns: Literature Review and an Integrative Framework. *Communications of the Association for Information Systems*, 28(28), pp. 453– 496.

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

Li, H., Sarathy, R., and Heng, X. (2010). Understanding situational online information disclosure as a privacy calculus. *Journal of Computer Information Systems,* 51(2). pp. 1-29.

Liao, C., Liu, C., and Chen, K. (2011). Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: An integrated model. *Electronic Commerce Research and Applications,* 10 (6), pp. 702-715.

Libaque-Saenz, C., Chang, Y., Kim, J., Park, M., and Rho, J. (2016). The role of perceived information practices on consumers' intention to authorise secondary use of personal data. *Behaviour and Information Technology,* 35 (5), pp. 339-356.

Liberty Mutual (2019). 2019 CSR Report. https://www.libertymutualgroup.com/documents/liberty-mutual-2019-esg-report-vfinal.pdf. [Accessed July 2021].

Liedong, T., Ghobadian. A., Rajwani, T., and O'Regan, N. (2015). Toward a View of Complementarity: Trust and Policy Influence Effects of CSRand Corporate Political Activity. *Group and Organization Management*, 40(3), pp. 405 –427.

Lincoln, Y., and Guba, E. (Eds. 1985). *Naturalistic Inquiry*. Thousand Oaks: Sage.

Lincoln, Y., Lynham, S., and Guba, E. (2011). Paradigmatic controversies, contradictions, and emerging confluences revisited. IN: K. Denzin and Y. S. Lincoln, *The SAGE handbook of qualitative research* (4th ed.). Thousand Oaks, CA: Sage, pp. 97–128.

Lind, E., and Tyler, T. (1988). *The social psychology of procedural justice.* New York : Plenum.

Linstone, H. (1978). The Delphi Technique. IN: R. Fowles, (ed.), *Handbook of Futures Research*, Greenwood Press, Westport, CT, pp.31-63.

Linstone, H., and Turoff, M. (1975). *The Delphi method. Techniques and applications*. Addison-Wesley Publishing Company Inc, Reading, M.A.

Linstone, H., and Turoff, M. (2002). *The Delphi method. Techniques and applications 2nd Ed*. Addison-Wesley Publishing Company Inc, Reading, M.A.

Litman, L., and Robinson, J. (2017). *Conducting Online Research on Amazon Mechanical Turk and Beyond*. SAGE Innovations in Research Methods

Liu, C., Marchewka, J., and Lu, C. (2005). Beyond concern – a privacy-trust-behavioural intention model of electronic commerce. *Information Management*, 42 (2), pp. 289-304.

Livingstone, S. (2008) Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media Society,* 10(3), pp. 393–411.

Lobera, J., Rodríguez, F., Torres-Albero, C. (2020). Privacy, values and machines: Predicting opposition to artificial intelligence. *Communication Studies*, 71(3), pp. 448-465.

Lobschat, L., Mueller, B., Eggers, F., and Brandimartee, L. (2021). Corporate digital responsibility. *Journal of Business Research,* 122(2), pp. 875-888.

Lock, I., and Seele, P. (2017). Measuring Credibility Perceptions in CSR Communication: A Scale Development to Test Readers' Perceived Credibility of CSR Reports. *Management Communication Quarterly*, 31(4), pp. 584–613.

Lock, I., and Seele, P. (2018). Politicized CSR: How corporate political activity (mis-)uses political CSR. *Journal of Public Affairs,* 18(3), pp. 1-9.

Lord, M. (2000). Constituency-based lobbying as corporate political strategy: Testing an agency theory perspective. *Business and Politics*, 2(3), pp. 289-308.

Loughlin K., and Moore L. (1979). Using Delphi to achieve congruent objectives and activities in a pediatrics department. *Journal of Medical Education*, 54, pp. 101-106.

Ludwig, B. (1994*). Internationalizing Extension: An exploration of the characteristics evident in a state university extension system that achieves internationalization.* Unpublished doctoral dissertation*,* The Ohio State University, Columbus.

Lundgren, B. (2020). A dilemma for privacy as control. *The Journal of Ethics*, 24(2), pp. 165–175.

Luo, R., Rajwani, T., Sun, P., Werner, T. and Doh, J. (2021). Call for Papers for a Special Issue. The Management of Sociopolitical Issues and Environments: Organizational and Strategic Perspectives. *Journal of Management Studies*, pp. 1-5.

Luo, X., and Bhattacharya, C. (2009). The Debate over Doing Good: Corporate Social Performance, Strategic Marketing Levers, and Firm-Idiosyncratic Risk. *Journal of Marketing,* 73(1), pp. 198–213.

Lux, S., Crook, T., and Woehr, D. (2011). Mixing business with politics: A meta-analysis of the antecedents and outcomes of corporate political activity. *Journal of Management*, 37, pp. 223-247.

Lwin, M., Wirtz, J., and Stanaland, A. (2016). The privacy dyad: Antecedents of promotion- and prevention-focused online privacy behaviours and the mediating role of trust and privacy concern. *Internet Research*, 26(4), pp. 919-941.

Lwin, M., Wirtz, J., and Williams, J. (2007). Consumer Online privacy concerns and Responses: A Power Equilibrium Model Perspective. *Journal of the Academy of Marketing Science*, 31(1), pp. 572-585.

Lynn, M., Laman, E., and Englebardt, S. (1998). Nursing administration research priorities: a national Delphi study. *Journal of Nursing Administration,* 28(5), pp. 7-11.

McDaniel, P., and Malone., R. (2012). The Big WHY": Philip Morris's Failed Search for Corporate Social Value. *American Journal of Public Health*, 102, pp. 1942–1950.

McKenna, H. (1994) The Delphi technique: a worthwhile approach for nursing? *Journal of Advanced Nursing,* 19, pp. 1221-1225.

McKinsey (2019). Answering society's call: A new leadership imperative. Available at https://www.mckinsey.com/business-functions/people-and-organizational-performance/our-insights/answering-societys-call-a-new-leadership-imperative. [Accessed August 2021].

McKinsey (2020). *Purpose-shifting from why to how*. Available at https://www.mckinsey.com/business-functions/people-and-organizational-performance/our-insights/purpose-shifting-from-why-to-how. [Accessed August 2021].

McKnight, D., and Chervany, N. (2002). What trust means in e-commerce customer relationships: an interdisciplinary conceptual typology. *International Journal of Electronic Commerce*, 6 (2), pp. 35-59.

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

McNall, L., and Stanton, J. (2011). Private Eyes Are Watching You: Reactions to Location Sensing Technologies. *Journal of Business and Psychology,* 26 (3), pp. 299-309.

McWilliams, A. (2015). Corporate Social Responsibility. IN: C. Cooper and J. Mcgee (eds), Wiley. *Encyclopedia of Management*, 12(1), pp. 1-9.

McWilliams, A., and Siegel, D. (2001). Corporate Social Responsibility: a Theory of the Firm Perspective. *Academy of Management Review*, 26(1), pp. 117-127.

McWilliams, A., Van Fleet, D., and Cory, K. (2002). Raising Rivals' Costs Through Political Strategy: An Extension of Resource-based Theory. *Journal of Management Studies*, 39(5), pp. 707-724.

Maier, A. (2021). Political corporate social responsibility in authoritarian contexts. *Journal of International Business Policy,* 4(1), pp. 476–495.

MacKenzie, S., Podsakoff, P. and Podsakoff, N. (2011). Construct measurement and validation procedures in MIS and behavioural research: Integrating new and existing techniques. *MIS Quarterly,* 35(2), pp. 293-334.

Makadok, R, Burton, and R, Barney, J. (2018). A practical guide for making theory contributions in strategic management. Strategic Management Journal, 39(1), pp. 1530– 1545.

Malhotra, N., Kim, S. and Agarwal, J. (2004). Internet Users' Information privacy concerns (IUIPC): The Construct, the Scale and a Causal Model. *Information Systems Research*, 15(4), pp. 336– 355.

Malhotra, N., Sahadev, S, and Purani, K. (2017). Psychological contract violation and customer intention to reuse online retailers: Exploring mediating and moderating mechanisms. *Journal of Business Research*, 75(1), pp. 17-28.

Malik, A; Hiekkanen, K.; Dhir, A., and Nieminen, M. (2016). Impact of privacy, trust and user activity on intentions to share Facebook photos. *Journal of Information, Communication and Ethics in Society,* 14 (4), pp. 364-382.

Mantelero, A. (2018). AI and Big Data: A blueprint for a human rights, social and ethical impact assessment. *Computer Law and Security Review*, 34(4), pp. 754-772.

Madsen, P., and Rodgers, Z. (2015). Looking good by doing good: The antecedents and consequences of stakeholder attention to corporate disaster relief. *Strategic Management Journal*, 36(5), pp. 776-794.

Mantere, S., Pajunen, K., and Lamberg, J. (2009). Vices and virtues of corporate political activity: The challenge of international business. *Business and Society*, 48(1), pp. 105–132.

Margulis, S. (1977). Conceptions of Privacy: Current Status and Next Steps. *Journal of Social Issues*, 33(3), pp. 5-21.

Margulis, S. (2003). Privacy as a Social Issue and Behavioral Concept. *Journal of Social Issues,* 59(2), pp. 243-261.

Martin, K. (2012). Diminished or Just Different? A Factorial Vignette Study of Privacy as a Social Contract. *Journal of Business Ethics*, 11(4), pp. 519-539.

Martin, K. (2013). Transaction costs, privacy, and trust: The laudable goals and ultimate failure of notice and choice to respect privacy online. *First Monday*. 18 (12): online.

Martin, K. (2016). Understanding privacy online: Development of a social contract approach to privacy. Journal of Business Ethics, 137 (3), pp. 551-569.

Martin, K. (2020). Breaking the Privacy Paradox: The Value of Privacy and Associated Duty of Firms. *Business Ethics Quarterly,* 30(1), 1-32.

Martin, K., and Murphy, P. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science,* 45(1), pp. 135-155.

Martin, K., and Nissenbaum, H. (2017). Measuring privacy: Using context to expose confounding variables. *Columbia Science and Technology Law Review*, pp. 1-40.

Martin, K., Borah, A., and Palmatier, R. (2017). Data Privacy: Effects on Customer and Firm Performance. *Journal of Marketing*, 81 (1), pp. 36-58.

Martin, K., Borah, A., and Palmatier, R. (2018). *Research: A Strong Privacy Policy Can Save Your Company Millions. Harvard Business Review.* Available at: https://hbr.org/2018/02/research-a-strong-privacy-policy-can-save-your-company-millions. [Accessed July 2021].

Martínez, P., and del Bosque, I. (2013). CSR and customer loyalty: the roles of trust, customer identification with the company and satisfaction. *International Journal of Hospitality Management*, 35(1), pp. 89-99.

Matten, D., and Crane, A. (2005). Corporate citizenship: toward an extended theoretical conceptualization. *Academy of Management Review,* 30(1), pp. 166–179.

Maxcy, S. (2003). Pragmatic Threads in Mixed Methods Research in the Social Sciences: The search for Multiple models of inquiry and the end of the Philosophy of Formalism. IN: Tashakkori, A. and Teddlie, C. (eds.) *Handbook of Mixed Methods in Social and Behavioral Research*, Thousand Oaks, CA: Sage Publications, pp. 51–90.

Maxwell, J. (1996). *Qualitative Research Design: An Interactive Approach*, Thousand Oaks, CA: Sage Publications.

Mayer, R., Davis, J., and Schoorman, F. (1995). An integrative model of organisational trust. *Academy of Management Review*, 20, pp. 709–734.

Mays, N., and Pope, C. (2000). Qualitative research in health care. Assessing quality in qualitative research. *BMJ (Clinical research ed.).* 320(7226), pp. 50–52.

Meinert, D., Peterson, D., Criswell, J., and Crossland, M. (2006). Privacy policy statements and consumer willingness to provide personal information. *Journal of Electronic Commerce in Organisations,* 4(1), pp. 1-17.

Melé, D. (2008). *Corporate social responsibility theories*. The Oxford handbook of corporate social responsibility. University Press, Oxford.

Mellahi, K., Frynas, J. G., Sun, P., Siegel, D. (2016). A review of the nonmarket strategy literature toward a multi-theoretical integration. *Journal of Management*, 42(1), pp. 143-173.

Menges, L. (2021). A Defense of Privacy as Control. *Journal of Ethics*, 25(1), pp. 385–402.

Merck (2019). 2019 CSR Report. https://www.merckgroup.com/en/cr-report/2019/. [Accessed July 2021].

Mertens, D. (2010). *Transformative research and evaluation*. New York: Guilford.

Meskaran, F., Ismail, Z., and Shanmugam, B. (2013). Online purchase intention: effects of trust and security perception. Australian Journal of Basic and Applied Sciences, 7(6), pp. 307-315.

–81.

Mesquita, L. (2007). Starting over when the bickering never ends: Rebuilding aggregate trust among clustered organisations through trust facilitators., *Academy of Management Review* 32(1), pp. 72-91.

Mezger, A., Cabanelas, P., López-Miguens, M., Cabiddu, F., and Rüdiger, K. (2020). Sustainable development and consumption: The role of trust for switching towards green energy. *Business Strategy and the Environment*, 29(1), pp. 3598–3610.

Microsoft (2019). 2019 CSR Report. https://www.microsoft.com/en-us/corporate-responsibility/reports-hub. [Accessed July 2021].

Microsoft (2020). *Microsoft blog: "Whatsapp Amicus Brief".* Available at: https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2020/12/NSO-v.-WhatsApp-Amicus-Brief-Microsoft-et-al.-as-filed.pdf. [Accessed July 2021].

Milberg, S., Smith, H., and Burke, S. (2000). Information Privacy: Corporate Management and National Regulation. *Organization Science*, 11(1), pp. 35–57.

Miles, M., and Huberman, A. (1994). *Qualitative data analysis: An expanded sourcebook (2nd ed.).* Sage Publications, Inc.

Miles, B., Hubermann, M., and Saldaña, J. (2013). *Qualitative Data Analysis: A Methods Sourcebook and The Coding Manual for Qualitative Researchers.* Thousand Oaks, CA: SAGE.

Milne, G. (2000). Privacy and Ethical Issues in Database/Interactive Marketing and Public Policy: A Research Framework and Overview of the Special Issue. *Journal of Public Policy and Marketing*, 19(1), pp. 1-6.

Milne, G., and Gordon, M. (1993). Direct Mail Privacy-Efficiency Trade-offs within an Implied Social Contract Framework. *Journal of Public Policy And Marketing*, 12(2), pp. 206–215.

Miller, L. (2006). Determining what could/should be: The Delphi technique and its application. Paper presented at the meeting of the 2006 annual meeting of the Mid-Western Educational Research Association, Columbus, Ohio.

Miller, T., and Triana, M. (2009). Demographic Diversity in The Boardroom: Mediators of the Board Diversity–Firm Performance Relationship. *Journal of Management Studies*, 46(5), pp. 755–86.

Miltgen, C., and Peyrat-Guillard, D. (2014). Cultural and generational influences on privacy concerns: a qualitative study in seven European countries. *European Journal of Information Systems,* 23(2), pp. 103 –125.

Milyo, J., Primo, D., and Groseclose, T. (2000). Corporate PAC campaign contributions in perspective. *Business and Politics*, 2(1), pp. 75–88.

Mirvis, P., and Googins, B. (2006). Stages of corporate citizenship. *California Management Review,* 48(2), pp. 104-26.

Mishra, S., and Modi, S. (2016). CSR and Shareholder Wealth: The Role of Marketing Capability. *Journal of Marketing*, 80(1), pp. 26–46.

Mitchell, A. (2018). A Review of Mixed Methods, Pragmatism and Abduction Techniques. *The Electronic Journal of Business Research Methods,* 16(3), pp. 103-116.

Mitchell, R., Agle, B., and Wood, D. (1997). Toward a theory of stakeholder identification and salience: defining the principle of who and what really counts. *Academy of Management Review*, 22(4), pp. 853-886.

Mohr, L., and Webb, D. (2005). The Effects of CSR and Price on Consumer Responses. *The Journal Of Consumer Affairs*, 39(1), pp. 121-147.

Montiel, I. (2008). CSR and Corporate Sustainability: Separate Pasts, Common Futures. *Organization and Environment*, 21(3), pp. 245-269.

Moon, J., Crane, A., and Matten, D. (2005). Can corporations be citizens? Corporate citizenship as a metaphor for business participation in society. *Business Ethics Quarterly*, 15(3), pp. 429-453.

Moor, J. (1997). Towards a Theory of Privacy in the Information Age. *Computers and Society*, 27(3), pp. 27-32.

Moore, A. (2003). Privacy: Its Meaning. *American Philosophical Quarterly*, 40(3), pp. 215– 227.

Moore, B. (1984*). Privacy: Studies in Social and Cultural history*. London: M.E. Sharpe.

Morgan, D. (2007). Paradigms Lost and Pragmatism Regained: Methodological Implications of Combining Qualitative and Quantitative Methods. *Journal of Mixed Methods Research*, 1(1), pp. 48-76.

Morhardt. E. (2010). Corporate social responsibility and sustainability reporting on the Internet. *Business Strategy and the Environment*, 19(7), pp. 436-452.

Morrison, B. (2013). Do We Know What We Think We Know? An Exploration of Online Social Network Users' Privacy Literacy. *Workplace Review*, 1, pp. 58—79.

Morse, J. (1997). Perfectly healthy, but dead: The myth of inter-rater reliability. *Qualitative Health Research,* 7(4), pp. 445–447.

Morse, J. (2003). Principles of Mixed Methods and MultiMethod Research Design. IN: Tashakkori, A. and Teddlie, C. (eds.) *Handbook of Mixed Methods in Social & Behavioral Research*, Thousand Oaks, CA: Sage Publications, pp. 189–208.

Morton, R., and Williams, K. (2010). *Experimental political science and the study of causality: From nature to the lab.* Cambridge; New York: Cambridge University Press.

Mosca, F. and Civera, C. (2017). The Evolution of CSR: An Integrated Approach*. SYMPHONYA Emerging Issues in Management,* 1, pp. 16-35.

Moss, A., and Litman, L. (2019). Demographics of people on Amazon Mechanical Turk. Available at https://www.cloudresearch.com/resources/blog/who-uses-amazon-mturk-2020-demographics/. [Accessed September 2021].

Mostellar, J., and Poddar, A. (2017). To Share and Protect: Using Regulatory Focus Theory to Examine the Privacy Paradox of Consumers' Social Media Engagement and Online Privacy Protection Behaviours. *Journal of Interactive Marketing*, 39(2), pp. 27-38.

Mothersbaugh, D., Foxx, W., Beatty, S., and Wang, S. (2012). Disclosure antecedents in an online service context: The role of sensitive information. *Journal of Services Research*, 15(1), pp. 76-98.

Mou, J., Shin, D., and Cohen, J. (2017). Trust and risk in consumer acceptance of e-services. *Electronic Commerce Research*, 17(2), pp. 255-288.

Mulaessa, N.; and Wang, H. (2017). The effect of corporate social responsibility (CSR) activities on consumers purchase intention in China: Mediating role of consumer support for responsible business*. International Journal of Marketing Studies*, 9(4), pp. 73-87.

Munilla, L., and Miles, M. (2005). The Corporate Social Responsibility Continuum as a Component of Stakeholder Theory, *Business and Society Review,* 110 (1), pp. 371-387.

Murphy, P., Laczniak, G., Bowie, N., and, Kleim, T. (2005). *Ethical Marketing.* Upper Saddle River, NJ : Pearson Publishing.

Murray, J., and Flyverbom, M. (2021). Datafied corporate political activity: Updating corporate advocacy for a digital era. Organization, 28(4), pp.621-640.

Murray, K., and Vogel, C. (1997). Using a hierarchy-of-effects approach to gauge the effectiveness of corporate social responsibility to generate goodwill toward the firm: Financial versus nonfinancial impacts. *Journal of Business Research*, 38(2), pp. 141-159.

Murray, W., and Jarman, B. (1987). Predicting future trends in adult fitness using the Delphi approach. *Research Quarterly for Exercise and Sport*, 58(2), pp. 124-131.

Mutimukwe, C., Kolkowska, E., and Grönlund, A. (2020). Information privacy in e-service: Effect of organizational privacy assurances on individual privacy concerns, perceptions, trust and self-disclosure behavior. *Government Information Quarterly,* 37(1), 101413.

Mutz, D. (2011). *Population-Based Survey Experiments.* Princeton, NJ: Princeton University Press.

Nadin, S., and Cassell, C. (2004). Using data matrices. In: Cassell C, editor; Symon G, editor. *Essential guide to qualitative research methods in organizational research*. Sage; London, pp. 271–287.

Nagle, F. , Seamans, R., and Tadelis, S. (2020). Transaction Cost Economics in the Digital Economy: A Research Agenda. *Harvard Business School Strategy Unit Working Paper*. 21(9).

Nalick, M., Josefy, M., Asghar, Z., and Bierman, L. (2016). Corporate Socio-Political Involvement: A Reflection of Whose Preferences? *Academy of Management Perspectives*, 30(4), 384-403.

Nasa, P., Jain, R., and Juneja, D. (2021). Delphi methodology in healthcare research: How to decide its appropriateness. *World Journal of Methodologies*, 11(4), pp.116-129.

Neuman, R. (2009). *Social Research Methods: Qualitative and Quantitative Approaches*. 7th Edition. Pearson Ed. Essex.

Newell, P. (1995). Perspectives on Privacy. *Journal of Environmental Psychology*, 15(2), pp. 87–104.

Newman, I., Ridenour, C., Newman, C. and DeMarco, G. (2003). A Typology of Research Purposes and its Relationship to Mixed Methods. IN: Tashakkori, A. and Teddlie, C. (eds.) *Handbook of Mixed Methods in Social and Behavioral Research*, Thousand Oaks, CA: Sage Publications, pp. 167–188.

Niederberger, M., and Spranger, J. (2020). Delphi Technique in Health Sciences: A Map. *Frontiers in Public Health,* 8(457), pp. 1-10.

Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford, CA: Stanford Law Books.

Nowell, L., Norris, J., and White, D. (2017). Thematic Analysis: Striving to Meet the Trustworthiness Criteria. *International Journal of Qualitative Methods*, 16(1), pp. 1-13.

Nunnally, J. (1967). *Psychometric theory.* New York McGraw-Hill.

Nunnally, J. (1978). *Psychometric theory*, *2nd ed.* New York: McGraw-Hill,

Nwagbara, U., and Belal, A. (2019) Persuasive language of responsible organisation? A critical discourse analysis of corporate social responsibility (CSR) reports of Nigerian oil companies. *Accounting, Auditing and Accountability Journal*, 32(8), pp. 2395-2420.

New York Times (2018). "Tech Industry Pursues a Federal Privacy Law, on Its Own Terms". Available at https://www.nytimes.com/2018/08/26/technology/tech-industry-federal-privacy-law.html. [Accessed November 2021].

New York Times (2021). “Google said it had successfully ‘slowed down’ European privacy rules, according to lawsuit”. Available at https://www.nytimes.com/2021/10/22/technology/google-privacy-lawsuit.html. [Accessed November 2021].

O’Cathain, A. (2010). Assessing the quality of mixed methods research: Toward a comprehensive framework. IN: Tashakkori A and Teddlie C (eds.) *Handbook of mixed methods in social and behavioural research. (2nd ed.)* Thousand Oaks, CA: Sage, pp 531-555.

O'Cathain A., Murphy, E., and Nicholl, J. (2008). The quality of mixed methods studies in health services research. *Journal of Health Service Research Policy,* 13(2), pp. 92-98.

O’Connor, T., and Hirsch, N. (1999). Intra-individual differences and relationship specificity of mentalising in early adolescence. *Social Development*, 8(2), pp. 256-274.

O'Neil, D. (2001). Analysis of internet users' level of online privacy concerns. *Social Science Computer Review,* 19 (1), pp. 17-31.

Oberman, W. (1993).Strategy and tactic choice in an institutional resource context. IN: Mitnick, B. M. (Ed.), *Corporate political activity*, Newbury Park, CA:Sage, pp. 213-241.

Okazaki, S., Li, H., and Hirose, M. (2013). Consumer privacy concerns and Preference for Degree of Regulatory Control. *Journal of Advertising*, 38(4), pp. 63-77.

Oliver, C., and Holzinger, I. (2008). The Effectiveness of Strategic Political Management: A Dynamic Capabilities Framework. The Academy of Management Review, 33(2), pp. 496–520.

Omarzu, J. (2000). A disclosure decision model: Determining how and when individuals will self-disclose. *Personality and Social Psychology Review*, 4(2), pp. 174-185.

Onwuegbuzie A., Bustamante R., and Nelson J. (2010). Mixed Research as a Tool for Developing Quantitative Instruments. *Journal of Mixed Methods Research*, 4(1), pp. 56-78.

Onwuegbuzie, A., and Collins, K. (2007). A Typology of Mixed Methods Sampling Designs in Social Science Research. *The Qualitative Report*, 12(2), pp. 281-316.

Onwuegbuzie, A., and Johnson, R. (2006). The “validity” issue in mixed research. *Research in the Schools,* 13(1), pp. 48–63.

Oracle (2019). 2019 CSR Report. https://www.oracle.com/a/ocom/docs/corporate/citizenship/ccr2019-report.pdf. [Accessed July 2021].

Ostas, D. (2007), The Law and Ethics of K Street: Lobbying, the First Amendment, and the Duty to Create Just Laws, *Business Ethics Quarterly*, 17(1), pp. 33-63.

Overall, J. (1993). Letter to the editor: The use of inadequate correlations for baseline imbalance remains a serious problem. *Journal of Biopharmaceutical Statistics*, 3(2), pp. 271-276.

Ozdoro-Aksak, E., and Atakan-Duman, S. (2016). Gaining legitimacy through CSR: an analysis of Turkey's 30 largest corporations. *Business Ethics: A European Review*, 25(3), pp. 238-257.

Ozer. M., and Alakent, E. (2012). The Influence of Ownership Structure on How Firms Make Corporate Political Strategy Choices. *Business and Society,* 52(3), pp. 451-472.

Paine, U., Reips, D., Stieger, S., Joinson, A., and Buchanan, T. (2007). Internet users' perceptions of ‘privacy concerns’ and ‘privacy actions’. *International Journal of Human-Computer Studies*, 65(6), pp. 526-536.

Palinkas, L., Horwitz, S., Green, C., Wisdom, J., Duan, N., and Hoagwood, K. (2015). Purposeful Sampling for Qualitative Data Collection and Analysis in Mixed Method Implementation Research. *Administration and policy in mental health,* 42(5), pp. 533–544.

Park, H., and Shin, G. (2004). *The Grand Unified Theory of the Firm and Corporate Strategy: Measures to build corporate competitiveness.* Korean Economic Research Institute, Seoul.

Park, J., Lee, H., and Kim, C. (2014). Corporate social responsibilities, consumer trust and corporate reputation: South Korean consumers' perspectives. *Journal of Business Research*, 67(3), pp. 295–302.

Pappas, I. (2018). User experience in personalized online shopping: a fuzzy-set analysis. *European Journal of Marketing, 5*2(7-8), pp. 1679-1703.

Parnell, J. (2019). Nonmarket and market strategies, strategic uncertainty and strategic capabilities: Evidence from the USA. *Management Research Review*, 41(2), pp. 252-274.

Patton, M. (2002). *Qualitative Research and Evaluation Methods, 3rd ed*. Thousand Oaks: Sage Publications.

Patton, M. (2015). *Qualitative Research and Evaluation Methods, 4th ed*. Thousand Oaks: Sage Publications.

Pavlou, P. (2003). Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model. *International Journal of Electronic Commerce*, 59(4), pp. 69-103.

Pavlou, P. (2011). State of the Information Privacy Literature: Where Are We Now and Where should we go? *MIS Quarterly,* 35(4), pp. 977–989.

Pavlou, P., and Gefen, D. (2004). Building effective online marketplaces with institution-based trust. *Information Systems Research,* 15(1), pp. 37–59.

Pavlou, P., and Fygenson, M. (2006). Understanding and Predicting Electronic Commerce Adoption: An Extension of the Theory of Planned Behavior. *MIS Quarterly*, 30(1), pp. 115-143.

Pavlou, P., Liang, H., and Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: a principal-agent perspective. *MIS Quarterly*, 31(1), pp. 105-136.

Peltzman, S. (1976). Toward a more general theory of regulation. *Journal of Law and Economics*, 19(1), pp. 211-240.

Pérez, A., and del Bosque, I. (2016). The stakeholder management theory of Corporate Social Responsibility: A multidimensional approach in understanding customer identification and satisfaction. *International Journal of Bank Marketing*, 34(1), pp. 731-751.

Pérez-Sindín, X. (2017). Secondary Data: sources, advantages and disadvantages. IN: Alen, M. (eds), *The Sage Encyclopedia of Communication Research Methods*. Thousand Oaks: Sage Publications, pp. 1578-1579.

Peterson, D., Meinert, D., Criswell, J., and Crossland, M. (2007). consumer trust: privacy policies and third-party seals. *Journal of Small Business and Enterprise Development*, 14(4), pp. 654-669.

PEW Research Centre (2015). *American attitudes about privacy, security and surveillance.* Available at: https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/. [Accessed June 2021].

PEW Research Centre (2016). *More Support for Justice Department Than for Apple in Dispute Over Unlocking iPhone*. Available at: https://www.pewresearch.org/topics/privacy-and-safety/project/u-s-politics/2016/. [Accessed June 2021].

PEW Research Centre (2018*). Americans' complicated feelings about social media in an era of privacy concerns*. Available at: ttps://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/. [Accessed August 2021].

Phelps, J., Nowak, G., and Ferrell, E. (2000). Privacy concerns and Consumer Willingness to Provide Personal Information. *Journal of Public Policy and Marketing*, 19(1), pp. 27-41.

Pirson, M., and Malhotra, D. (2011). Foundations of Organizational Trust: What Matters to Different Stakeholders? *Organization Science*, 22(4), pp. 1087-1104.

Pirson, M., Martin, K., and Parmar, B. (2017). Formation of Stakeholder Trust in Business and the Role of Personal Values. Journal of Business Ethics, 145(1), pp. 1-20.

Pivato, S., Misani, N., and Tencati, A. (2008). The Impact of CSR on consumer trust: the Case of Organic Food. *Business Ethics: A European Review*, 17(1), pp. 3-12.

Podsakoff, P., MacKenzie, S., Lee, J., and Podsakoff, N. (2003). Common method biases in behavioural research: a critical review of the literature and recommended remedies. *The Journal of Applied Psychology,* 88(5), pp. 879–903.

Podsakoff, N., Whiting, S., Podsakoff, P., and Mishra, P. (2011). Effects of organizational citizenship behaviours on selection decisions in employment interviews. *Journal of Applied Psychology,* 96(2), pp. 310-326.

Polit, D., and Tatano-Beck, C. (2010). Generalization in quantitative and qualitative research: Myths and strategies. *International Journal of Nursing Studies,* 47 (1), pp. 1451–1458.

Polit, D., and Hungler, B. (1997). *Essentials of Nursing Research: Methods, Appraisal and Utilisation.* Lippincott, New York.

Pollach, I. (2011). Online privacy as a corporate social responsibility: an empirical study. *Business Ethics: A European Review*, 20(1), pp. 88-103.

Porter, M., and Kramer, M. (2011). The Big Idea: Creating Shared Value. How to Reinvent Capitalism—and Unleash a Wave of Innovation and Growth. *Harvard Business Review,* 89(1-2), pp. 62-77.

Posey, C., Lowry, P., Roberts, T., and Ellis, S. (2010). Proposing the online community self-disclosure model: The case of working professionals in France and the UK who use online communities. *European Journal of Information Systems*, 19(2), pp. 181–195.

Pratt, M., Kaplan, S., and Whittington, R. (2020). Editorial essay: The tumult over transparency: Decoupling transparency from replication in establishing trustworthy qualitative research. *Administrative Science Quarterly*, 65(1), pp. 1-19.

Preibusch, S., Kübler, D., and Beresford, A. (2013). Price versus privacy: an experiment into the competitive advantage of collecting less personal information. *Electronic Commerce Research*, 13(1), pp. 423–455.

Preston, L. (1998). Agents, stewards, and stakeholders. *Academy of Management Review*, 23(1), pp. 1–9.

Price, P., Jhangiani, R., and Chiang, I. (2015*). Research Methods of Psychology – 2nd Edition*. Victoria, B.C.

Privacy Rights Clearinghouse (2021). *Data breaches*. Available at https://privacyrights.org/data-breaches. [Accessed September 2021].

Proton Technologies (2019). Do consumers know their GDPR data privacy rights? Available at https://gdpr.eu/consumers-gdpr-data-privacy-rights/. [Accessed November 2021]

Punch, K. (2005). *Introduction to social research: Quantitative and qualitative approaches (2nd ed.).* Thousand Oaks, CA: Sage.

Raab, C. (2020). Information privacy, impact assessment, and the place of ethics∗. *Computer Law and Security Review*, 37(1).105404, pp. 1-16.

Rachels, J. (1975). Why privacy is important. *Philosophy and Public Affairs*, 4(4), pp. 323–333.

Rajwani, T., and Liedong T. (2015) Political activity and firm performance within nonmarket research: a review and international comparative assessment. *Journal of World Business,* 50(1), pp. 273–283.

Redish, M. (1982). Value of Free Speech. *130U Pennsylvania Law Review*, 591.

Regan, P., Fitzgerald, G. and Balint, P. (2013). Generational views of information privacy? Innovation: *The European Journal of Social Science Research*, 26(1-2), pp. 81–99.

Reed, M. (2005). Reflections on the 'realist turn' in organisation and management studies. *Journal of Management Studies*, 42(8), pp. 1621–1644.

Reuters (2016). *Apple 'privacy czars' grapple with internal conflicts over user data*. Available at: . https://www.reuters.com/article/us-apple-encryption-privacy-insight/apple-privacy-czars-grapple-with-internal-conflicts-over-user-data-idUSKCN0WN0BO. [Accessed June 2021].

Richter, B. (2011*).*"Good" and "evil": The relationship between corporate social responsibility and corporate political activity. *SSRN Electronic Journal, DOI:10.2139/ssrn.1750368.*

Ritchie, J., and Lewis, J. (eds.)(2003). *Qualitative Research Practice: A Guide For Social Science Students and Researchers.* Sage Publications.

Rodriguez, P., Siegel, D., Hillman, A., Eden, L. (2006). Three lenses on the multinational enterprise: Politics, corruption, and corporate social responsibility. *Journal of International Business Studies,* 37(1), pp. 733-746.

Rosenbloom, A., and Haefner, J. (2009). Country-of-Origin Effects and Global Brand Trust: A First Look. *Journal of Global Marketing*, 22(4), pp. 267-278.

Rogers, M., and Lopez, E. (2002). Identifying critical cross-cultural school psychology competencies. *Journal of School Psychology*, 40(2), pp. 115-141.

Rousseau, D., Sitkin, S., Burt, R., and Camerer, C. (1998). Introduction to special topic forum: Not so different after all: A cross-discipline view of trust. *Academy of Management Review,* 23(3), pp. 393-404.

Rudy, B, and Cavich, J. (2017). Nonmarket Signals: Investment in CPA and the Performance of Initial Public Offerings. *Business and Society*, 59(3), pp. 419-438.

Rust, R., Kannan, P., and Peng, N. (2002). The customer economics of Internet privacy. *Academy of Marketing Science,* 30(4), pp. 455-468.

Ryan, G., and Bernard, H. (2000). Data management and analysis methods. IN: Denzin, N., Lincoln, Y. (Eds.), *Handbook of qualitative research* (2nd ed.),Thousand Oaks, CA: Sage, pp. 769–802.

Saisana, M. and Tarantola, S. (2002). *State-of-the-art report on current methodologies and practices for composite indicator development.* Report EUR 20408 EN. European Commission–Joint Research Centre, Ispra. Available at: https://www.eea.europa.eu/data-and-maps/indicators/economic-water-productivity-of-irrigated/state-of-the-art-report. [Accessed July 2021].

Salesforce (2018). *Business as a platform for change*. *Salesforce CEO Marc Benioff Calls for National Privacy Law*. Available at: https://www.salesforce.com/news/stories/salesforce-ceo-marc-benioff-calls-for-national-privacy-law/. [Accessed July 2021].

Sandelowski, M. (1995). Sample size in qualitative research. *Research in Nursing and Health*. 18(2), pp. 172-183.

SANS (2018). *Data Protection – EU vs US Definition*. Available at https://www.sans.org/blog/data-protection-eu-vs-us-definition/. [Accessed September 2021].

SaratChandran, P. (2005). Workplace Privacy and CSR. Australian Law Reform Commission Reform Journal 4930; 87.

Saunders, M., Lewis, P., and Thornhill, A. (2007). *Research methods for Business Students* (4th ed.): London: Prentice Hall.

Saunders, M., Lewis, P., and Thornhill, A. (2015*). Research Methods for Business Students.* England: *Journal of Futures Studies.* Pearson Education Limited.

Saunders, M., Lewis, P., Thornhill, A., and Bristow, A. (2019). Understanding research philosophy and approaches to theory development. IN, *Research Methods for Business Students,* Pearson Education. Chapter 4, pp. 128-171.

Sen, S., and Bhattacharya, C. (2001). Does doing good always lead to doing better? Consumer reactions to corporate social responsibility. Journal of Marketing Research, 38(2), pp. 225–243.

SaratChandran, P. (2005). Workplace Privacy and CSR. Australian Law Reform Commission Reform Journal 4930; 87.

Savitz, A. (2013). *The Triple Bottom Line: How Today's Best-Run Companies Are Achieving Economic, Social and Environmental Success - and How You Can Too*. Jossey-Bass Press, San Francisco, CA.

Scariano, S., and Davenport, J. (1987). The Effects of Violations of Independence Assumptions in the One-Way ANOVA. *The American Statistician,* 41(2), pp. 123-129.

Schaerer, M, du Plessis, C., Yap, A., and Thau, S. (2018). Low power individuals in social power research: A quantitative review, theoretical framework, and empirical test. *Organizational Behavior and Human Decision Processes*, 149(2), pp. 73-96.

Scherer, A. (2018). Theory Assessment and Agenda Setting in Political CSR: A Critical Theory Perspective. *International Journal of Management Reviews*, 20(1), pp. 387–410.

Scherer, A., Rasche, A., and Palazzo, G. (2016). Managing for Political CSR- New Challenges and Directions for PCSR 2.0. *Journal of Management Studies*, 53(3), pp. 273-298.

Scherer, A., and Palazzo, G. (2011). The New Political Role of Business in a Globalized World: A Review of a New Perspective on CSR and its Implications for the Firm, Governance, and Democracy. *Journal of Management Studies*, 48(4), pp. 900-931.

Schillemans, T., and Busuioc, M. (2015). Predicting Public Sector Accountability: From Agency Drift to Forum Drift. *Journal of Public Administration Research and Theory,* 25(1), pp. 191-215.

Schoder, D., and Haenlein, M. (2004). The relative importance of different trust constructs for sellers in the online world. *Electronic Markets*, 14(1), pp. 48-57.

Schuh, S. , Van Quaquebeke, N., Keck, N., Göritz, A., Cremer, D., and Xin, K. (2018). Does it Take More Than Ideals? How Counter-Ideal Value Congruence Shapes Employees' Trust in the Organization. Journal of Business Ethics, 149(4), pp. 987-1003.

Schultz, S., and Seele, P. (2019) Conceptualizing data-deliberation: The starry sky beetle, environmental system risk, and Habermasian CSR. *Business ethics*, 29(2), pp. 303-313.

Seele, P., and Lock, I. (2015). Instrumental and/or Deliberative? A Typology of CSR Communication Tools. *Journal of Business Ethics,* 131(2), pp. 401– 414.

Sekaran, U. (2003). *Research Methods for Business: A Skill-Building Approach. 4th Edition*, John Wiley and Sons, New York.

Sekayi, D., and Kennedy, A. (2017). Qualitative Delphi Method: A Four Round Process with a Worked Example. *The Qualitative Report*, 22(10), pp. 2755-2763.

Seltman, H. (2018). Experimental Design and Analysis. Carnegie Mellon University Press. Available at http://www.stat.cmu.edu/~hseltman/309/Book/Book.pdf. [Accessed November 2021].

Sen, S., and Bhattacharya, C. (2001). Does doing good always lead to doing better? Consumer reactions to corporate social responsibility. Journal of Marketing Research, 38(2), pp. 225–243.

Sen, S., Bhattacharya, C., and Korschun, D. (2006). The role of corporate social responsibility in strengthening multiple stakeholder relationships: A field experiment. *Journal of the Academy of Marketing Science,* 34(2), pp. 158–166.

Senn, S. (1994). Testing for baseline balance in clinical trials. *Statistics in Medicine,* 13(17), pp. 1715-1726.

Senn, S. (2006). Change from baseline and analysis of covariance revisited. *Statistics in Medicine*, 25(24), pp. 4334–4344.

Shannon-Baker, P. (2015) Making Paradigms Meaningful in Mixed Methods Research. *Journal of Mixed Methods Research,* 32, pp. 1-16.

Shariff, N. (2015). Utilizing the Delphi Survey Approach: A Review. *Journal of Nursing Care*, 4(3), pp. 246-251.

Sharma, R., Ng, E., Dharmawirya, M., and Lee, C. (2008). Beyond the digital divide: a conceptual framework for analyzing knowledge societies. *Journal of Knowledge Management*, 12(5), pp. 151-164.

Sheehan, K., and Hoy, M. (2000). Dimensions of privacy concern among online consumers. *Journal of Public Policy and Marketing,* 19 (1), pp. 62-73.

Sheehy, B. (2015). Defining CSR: Problems and Solutions. *Journal of Business Ethics*, 131(3), pp. 625–648.

Sheehy, B.; and Farneti, F. (2021). Corporate Social Responsibility, Sustainability, Sustainable Development and Corporate Sustainability: What Is the Difference, and Does It Matter? *Sustainability,* 13, 5965.

Shilton, K., and Greene, D. (2019). Linking Platforms, Practices, and Developer Ethics: Levers for Privacy Discourse in Mobile Application Development. *Journal of Business Ethics,* 155(1), pp.131-146.

Shirodkar, V., Beddewela, E., and Richter, U. (2018). Firm-Level Determinants of Political CSR in Emerging Economies: Evidence from India. *Journal of Business Ethics,* 148(3), pp. 673–688.

Shirodkar, V., and Mohr, A. (2015). Resource Tangibility and Foreign Firms' Corporate Political Strategies in Emerging Economies: Evidence from India. *Management International Review*,

Siegel, D. (2009). Green management matters only if it yields more green: An economic/strategic perspective. *Academy of Management Perspectives*, 23(3), pp. 5-16.

Sitkin, S., and Roth, N. (1993). Explaining the limited effectiveness of legalistic 'remedies' for trust/distrust. *Organisation Science,* 4(3), pp. 367-392.

Skulimowski, A. (2017). Expert Delphi Survey as a Cloud-Based Decision Support Service. *Proceedings of the 2017 IEEE 10th Conference on Service-Oriented Computing and Applications (SOCA), Kanazawa,* pp. 190-197.

Skulmoski, G., Hartman, F., and Krahn, J. (2007). The Delphi Method for Graduate Research. *Journal of Information Technology Education.* 6(1), pp. 1-21.

Sen, S., Bhattacharya, C., and Korschun, D. (2006). The Role of CSR in Strengthening Multiple Stakeholder Relationships: A Field Experiment. *Journal of the Academy of Marketing Science*, 34(2), pp. 158-166.

Skinner, R.; Nelson, R., Chin, W., and Land, L. (2015). The Delphi Method Research Strategy in Studies of Information Systems. *Communications of the Association for Information Systems*: 37(2), pp. 31-63.

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

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

Solove, D. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review,* 154(3), pp. 477–564.

Solove, D. (2007). I've Got Nothing to Hide' and Other Misunderstandings of Privacy. *San Diego Law Review, 44, 745. GWU Law School Public Law Research Paper No. 289*.

Son, J., and Kim, S. (2008). Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model. *MIS Quarterly,* 32(3), pp. 503–529.

Son, J., and Park, J. (2016). Procedural justice to enhance compliance with non-work-related computing (NWRC) rules: Its determinants and interaction with privacy concerns. *International Journal of Information Management,* 36(3), pp. 309-321.

Spector, P., and Brannick, M. (2011). Methodological Urban Legends: The Misuse of Statistical Control Variables. *Organizational Research Methods*, 14(2), pp. 287-305.

Spence, L., Coles, A., and Harris, L. (2001). The Forgotten Stakeholder? Ethics and Social Responsibility in Relation to Competitors. *Business and Society Review,* 106(4), pp. 331–352.

Steiner, P., Atzmüller, C. and Su, D. (2016). Designing Valid and Reliable Vignette Experiments for Survey Research: A Case Study on the Fair Gender Income Gap. *Journal of Methods and Measurement in the Social Sciences*, 7(2), pp. 52-94.

Statistica (2021). Number of subscribers to wireless carriers in the U.S. from 1st quarter 2013 to 2nd quarter 2020, by carrier. Available at https://www.statista.com/statistics/283507/subscribers-to-top-wireless-carriers-in-the-us/. [Accessed November 2021].

Stigler, G. (1971). The theory of economic regulation. *Bell Journal of Economics and Management Science*, 2(1), pp. 3-21.

Storey, V., Kane, G., and Schwaig, K. (2009). The Quality of Online Privacy Policies: A Resource Dependency Perspective. *Journal of Database Management*, 20(2), pp. 19-27.

Straub, D., Boudreau, M., and Gefen, D. (2004). Validation Guidelines for IS Positivist Research. *Communications of the AIS*, 13(24), pp. 380-427.

Swaen, V., and Chumpitaz, R. (2008). Impact of corporate social responsibility on consumer trust. *Recherche et Applications en Marketing*, 23(4), pp. 7-34.

Swaminathan, V., Sorescu, A., Steenkamp, J., Clayton Gibson O'Guinn T., and Schmitt, B. (2020). Branding in a Hyperconnected World: Refocusing Theories and Rethinking Boundaries. *Journal of Marketing*, 84 (2), pp. 24–46.

Alashoor, T., Han, S., and Joseph, R. (2017). Familiarity with Big Data, Privacy Concerns, and Self-disclosureAccuracy in Social Networking Websites: An APCO Model. *Communications of the Association for Information Systems*, 41(4), pp. 62-96.

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

Talhelm, T., Haidt, J., and Oishi, S. (2015). Liberals Think More Analytically (More "WEIRD") Than Conservatives. *Personality and Social Psychology Bulletin*, 41(2), pp. 250–267.

Tashakkori, A., and Teddlie, C. (1998). *Mixed Methodology: Combining Qualitative and Quantitative Approaches.* Thousand Oaks, CA: Sage Publications.

Tashakkori, A., and Teddlie, C. (2008). Quality of Inferences in Mixed Methods Research: Calling for an Integrative Framework. IN: Bergman, M. (ed.) *Advances in Mixed Methods Research: Theories and Applications*. London: Sage Publications, pp. 101-119.

Tate, W., Ellram, L., and Kirchoff, J. (2010). Corporate social responsibility reports: A thematic analysis related to supply chain management. *Journal of Supply Chain Management*, 46(1), pp. 19–44.

Tavani, H. (2000). Defining the boundaries of computer crime: piracy, break-ins, and sabotage in cyberspace. *ACM SIGCAS Computers and Society*, 30(3), pp. 3-9.

Tavani H. (2008). Informational Privacy: Concepts, Theories, and Controversies. IN: K. Himma, H. Tavani (eds) *The Handbook of Information and Computer Ethics*. Hoboken, NJ: John Wiley and Sons, pp.131–164.

Taylor, D., Davis, D., and Jillapal, R. (2009). privacy concern and online personalization: the moderating effects of information control and compensation. *Electron Commerce Research*, 9(3), pp. 203–223.

Taylor E. (2019). We Agree, Don't We? The Delphi Method for Health Environments Research. *HERD: Health Environments Research & Design Journal*. 13(1), pp. 11-23.

Teddlie, C., and Tashakkori, A. (2009). *Foundations of mixed methods research: Integrating quantitative and qualitative approaches in the social and behavioural sciences*. Thousand Oaks, CA: Sage

Tesler, L., and Malone. R. (2008). Corporate Philanthropy, Lobbying, and Public Health Policy. *American Journal of Public Health*, 98(1), pp. 2123–2133.

Thakur, R., and Srivastava, M. (2014). Adoption readiness, personal innovativeness, perceived risk and usage intention across customer groups for mobile payment services in India. *Internet Research,* 24(3), pp. 369-392.

Thibaut, J., and Walker, L. (1975). *Procedural justice: A psychological analysis*. Hillsdale , NJ : Lawrence Erlbaum Associates.

Thompson, N., McGill, T., Bunn, A., and Alexander, R. (2020). Cultural factors and the role of privacy concerns in acceptance of government surveillance. *Journal of the Association for Information Science and Technology*, 71(9), pp. 1129–1142.

Thorne, S. (2000). Data analysis in qualitative research. *Evidence Based Nursing*, 3(2), pp. 68–70.

Timans, R., Wouters, P., and Heilbron, J. (2019). Mixed methods research: what it is and what it could be. *Theory and Society*, 48 (2), pp. 193-216.

Tomlinson, E., Lewicki, R. and Ash, S. (2014). Disentangling the moral integrity construct: Values congruence as a moderator of the behavioural integrity–citizenship relationship. *Group and Organization Management,* 39(6), pp. 720-743.

Trapp, N. (2012). Corporation as climate ambassador: Transcending business sector boundaries in a Swedish CSR campaign. *Public Relations Review*, 38(3), pp. 458–465.

Tobin, G., and Begley, C. (2004). Methodological rigor within a qualitative framework. *Journal of Advanced Nursing*, 48(4), pp. 388-96.

Toma, C., and Picioreanu, J. (2016). The Delphi Technique: Methodological Considerations and the Need for Reporting Guidelines in Medical Journals. *International Journal of Public Health Research,* 4(6), pp. 47-59.

Tortosa-Edo, V., and López-Navarro, M. (2020). How do perceived CPA and political CSR interact in their relationships with citizens' trust in companies? *Social Responsibility Journal*. (ahead of print).

Tost. L. (2015). When, why, and how do powerholders "feel the power"? Examining the links between structural and psychological power and reviving the connection between power and responsibility. *Research in Organizational Behavior*, 35(1), pp. 29-56.

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., Lind, F. (2015). Do people know about privacy and data protection strategies? Towards the "Online Privacy Literacy Scale" (OPLIS). In. S. Gutwirth, R. Leenes & P. de Hert (Eds.). Reforming European Data Protection Law. (pp. 333-365). Springer Netherlands.

Trüdinger, E., and Steckermeier, L. (2017). Trusting and controlling? Political trust, information and acceptance of surveillance policies: The case of Germany. *Government Information Quarterly,* 34(3), pp. 421–433.

Tsai, J., Egelman, S., Cranor, L., and Acquisti, A. (2010). The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. *Information Systems Research,* 22 (2), pp. 254-268.

Tsai, J., Joe, S., Lin, C., Chiu, C., and Shen, K. (2015). Exploring corporate citizenship and purchase intention: mediating effects of Brand trust and corporate identification. *Business Ethics*: *A European Review*, 24(4), pp. 361-377.

Tsarenko, Y., and Tojib, D. (2009). Examining customer privacy concerns in dealings with financial institutions. *Journal of Consumer Marketing*, 26 (7), pp. 468-476.

Tucker, C. (2014). The reach and persuasiveness of viral video ads. *Marketing Science*, 34 (2), pp. 281-296.

Turel, O., Yuan, Y., and Connelly, C. (2008) In justice we trust: Predicting user acceptance of e-customer services. *Journal of Management Information Systems,* 24(4), pp. 123–151.

Unerman, J. (2000). Reflections on Quantification in Corporate Social Reporting Content Analyses. Accounting. *Auditing and Accountability Journal*, 13(1), pp. 667-681.

United Health (2019). 2019 CSR Report. https://www.unitedhealthgroup.com/viewer.html?file=/content/dam/UHG/PDF/2019/SR-Report-2018-Q4.pdf. [Accessed July 2021].

Vaismoradi, M., Jones, J., Turunen, H. and Snelgrove, S. (2016). Theme development in qualitative content analysis and thematic analysis. *Journal of Nursing Education and Practice,* 6(1), pp. 100-110.

Vaismoradi, M., Turunen, H., and Bondas, T. (2013). Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study. *Nursing and Health Sciences*,15 (2), pp. 398–405.

Valente, M., and Crane, A. (2010). Public responsibility and private enterprise in developing countries. *California Management Review*, 52(3), pp. 52-78.

Valero (2019). 2019 CSR Report. https://www.responsibilityreports.com/HostedData/ResponsibilityReports/PDF/NYSE_VLO_2019.pdf. [Accessed July 2021].

Van Dijk, M., van Herk, H., and Prins, R. (2019). Choosing your charity: the importance of value congruence in two-stage donation choices. *Journal of Business Research*, pp. 283-292.

Van Dyke, T., Vishal, M., and Nemati, H. (2007). The effect of consumer privacy empowerment on trust and privacy concerns in e-commerce. *Electronic Markets*, 17(1), 105(4), pp. 68–81.

Van Marrewijk, M. (2003). Concepts and definitions of CSR and Corporate Sustainability: between Agency and Communion. *Journal of Business Ethics*, 44(2), pp. 95-105.

Van Marrewijk, M., and Were, M. (2003). Multiple Levels of Corporate Sustainability. *Journal of Business Ethics*, 44(2), pp. 107-119.

Varkonyi, G., Kertesz, A., Varadi, S. (2019). Privacy-awareness of Users in our Cloudy Smart World. *Proceedings of the Fourth International Conference on Fog and Mobile Edge Computing (FMEC)*, pp. 189-196.

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

Verizon (2019). 2019 CSR Report. https://www.verizon.com/about/sites/default/files/esg-report/2019/Verizon-2019-ESG-Report.pdf. [Accessed July 2021].

Verizon (2021). *2021 Data breach Investigations Report*. Available at: https://www.verizon.com/business/resources/reports/dbir/. [Accessed August 2021].

Visser, W. (2010). The age of responsibility: CSR 2.0 and the new DNA of business. *Journal of Business Systems, Governance and Ethics,* 5(3), pp. 7– 22.

Vlachos, P., Theotokis, A. and Panagopoulos, N. (2010). Sales force reactions to corporate social responsibility: attributions, outcomes, and the mediating role of organisational trust. *Industrial Marketing Management,* 39(7), pp. 1207-1218.

Voegtlin, C., Frisch, C., Walther, A., and Schwab, P. (2019). Theoretical Development and Empirical Examination of a Three-Roles Model of Responsible Leadership. *Journal of Business Ethics*, 167(5), pp. 1-49.

Vogt, W. (2005). *Dictionary of Statistics and Methodology: A Nontechnical Guide for the Social Sciences*. SAGE.

Voinea C., and van Kranenburg, H. (2018). Feeling the Squeeze: Nonmarket Institutional Pressures and Firm Nonmarket Strategies. *Management International Review*, 58(5), pp. 705-741.

Von der Gracht, H. (2012) Consensus measurement in Delphi studies. Review and implications for future quality assurance. *Technological Forecasting and Social Change,* 79(8), pp. 1525-1536.

VpnMentor (2019). *The issues that matter to The Big Tech Lobby* Available at: https://www.vpnmentor.com/research/us-lobby-report/. [Accessed August, 2021].

Vredenburg, J., Kapitan, S., Spry, A., and Kemper, J. (2020). Brands Taking a Stand: Authentic Brand Activism or Woke Washing? *Journal of Public Policy and Marketing,* 39(4), pp. 1-50.

Waddock, S., and McIntosh, M. (2011). Business Unusual: Corporate Responsibility in a 2.0 World. *Business and Society Review*, 116(3), pp. 303-330.

Wakefield, R. (2013). The influence of user affect in online information disclosure. *The Journal of Strategic Information Systems*, 22(2), pp.157-174.

Waldman, A. (2018). *Privacy as Trust: Information Privacy for an Information Age.* New York Law School. Cambridge University Press.

Waldo, J., Lin, H., and Millett, L. (2007). Engaging Privacy and Information Technology in a Digital Age. Committee on Privacy in the Information Age, National Research Council.

Walsham, G. (1995). Interpretive Case Studies in IS Research: Nature and Method. *European Journal of Information Systems,* 4 (2), pp. 74-81.

Warner, M., and Wang, V. (2019). Self-censorship in social networking sites (SNSs) - privacy concerns, privacy awareness, perceived vulnerability and information management. *Journal of Information Communications and Ethics in Society,* 17(1), pp. 375-394.

Warren, S., and Brandeis, L. (1890). The Right to Privacy. *Harvard Law Review*, 4(5), pp. 193-220.

Wartick, S., and Cochran, P. (1985). The evolution of the corporate social performance model. *Academy of Management Review*, 10(4), pp. 758-769.

Weber, J. (1992). Scenarios in business ethics research: A review, critical assessment, and recommendations. *Business Ethics Quarterly,* 2(2), pp. 137–160.

Weber-Shandwick. (2018). CEO Activism in 2018: The Purposeful CEO. Available at https://www.webershandwick.com/wp-content/uploads/2018/07/CEO-Activism-2018_Purposeful-CEO.pdf. [Accessed November 2021].

Weingarten, F., Pagell, M., and Fynes, B. (2012). Supply chain environmental investments in dynamic industries: Comparing investment and performance differences with static industries. *International Journal of Production Economics,* 135(2), pp. 541–51.

Werner, T. (2017). Investor Reaction to Covert CPA. *Strategic Management Journal*, 38(12), pp. 2424–2443.

West, S., Aiken, L., and Krull, J. (1996). Experimental personality designs: Analyzing categorical by continuous variable interactions. *Journal of Personality*, 64(1), pp. 1–48.

Westin, A. (1967). *Privacy and Freedom.* New York: Athenbaum.

Westin, A. (2003). Social and Political Dimensions of Privacy. *Journal of Social Issues*, 59(2), pp. 431–453.

Whitman, N. (1990). The committee meeting alternative: using the Delphi technique. *Journal of Nursing Administration,* 20(7), pp. 30-37.

Whittier, N., Wildhagen, T., and Gold, H. (2019). *Statistics for Social Understanding: With Stata and SPSS*. Rowman and Littlefield Publishing.

Wiengarten, F., Fan, D., Pagell, M. and Lo, C. (2019). Deviations from aspirational target levels and environmental and safety performance: Implications for operations managers acting irresponsibly. *Journal of Operations Management*, 65 (6), pp. 490-516.

Wiengarten, F., Pagell, M., and Fynes, B. (2012). Supply chain environmental investments in dynamic industries: Comparing investments and performance differences with static industries. *International Journal of Production Economics*, 135 (2), pp. 541-551.

Wirtz, J., and Lwin, M. (2009). Regulatory Focus Theory, Trust, and privacy concern. *Journal of Service Research*. 12(2), pp. 190-207.

Wissinger, C. (2017). Privacy literacy: From theory to practice. *Communications in Information Literacy,* 11(2), pp. 378-389.

Witkin, B. (1984). *Assessing needs in educational and social programs*. San Francisco, CA: Jossey-Bass Publishers.

Wood, D., and Logsdon, J. (2008). Business Citizenship as Metaphor and Reality. *Business Ethics Quarterly,* 18(1), pp. 51-59.

World Medical Association (2013).Declaration of Helsinki: Ethical Principles for Research Involving Human Subjects.JAMA.310(20), pp. 2191–2194.Available at https://web.archive.org/web/20091015082020/http://www.wma.net/en/30publications/10policies/b3/index.html. [Accessed September 2021].

Worrell, J., Di Gangi, P, and Bush, A. (2013). Exploring the use of the Delphi method in accounting information systems research. *International Journal of Accounting Information Systems,*14(3), pp. 193–208.

Wright, S. and Xie, G. (2019). Perceived Privacy Violation: Exploring the Malleability of Privacy Expectations. *Journal of Business Ethics*, 156(1), pp.123-140.

Wrona, T., and Sinzig, C. (2018). Nonmarket strategy research: systematic literature review and future directions. *Journal of Business Economics*, 88 (1), pp. 253–317.

Wu, K., Huang, S., Yen, D., and Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior*, 28(3), pp. 889-897.

Xu, H. (2007). The Effects of Self-Construal and Perceived Control on privacy concerns. *Proceedings of the 28th International Conference on Information Systems,* Montréal, Canada.

Xu, H. (2009). Consumer Responses to the introduction to privacy protection measures: an exploratory research framework. *International Journal of E-Business Research,* 5(2), pp.161-189.

Xu, H., Dinev, T., Smith, J. and Hart, P. (2008). Examining the Formation of Individual's privacy concerns: Toward an Integrative View. *29th International Conference on Information Systems*.

Xu, H., Dinev, T., Smith, J., and Hart, P. (2011). Information privacy concerns: Linking Individual Perceptions with Institutional Privacy Assurances. *Journal of the Association for Information Systems*,12(2), pp. 798-824.

Xu, H., Teo, H., Tan, B., and Agarwal, R. (2012). Effects of Individual Self-Protection, Industry Self-Regulation, and Government Regulation on privacy concerns: A Study of Location-Based Services*. Information Systems Research*, 23(4), pp. 1342-1363.

Xueming, L. (2002). Trust production and privacy concerns on the Internet: A framework based on relationship marketing and social exchange theory. *Industrial Marketing Management*, 31(2), pp. 111-118.

Yang, C., Huang, Q., Li, Z., Liu, K., and Hu, F. (2017). Big Data and cloud computing: innovation opportunities and challenges. *International Journal of Digital Earth*, 10(1), pp.13-53.

Yardley, L. (2008). Demonstrating the validity of qualitative research. *The Journal of Positive Psychology,* 12 (2), pp. 295-296.

Yu, H., Jiang, S., and Land, K. (2015). Multicollinearity in Hierarchical Linear Models. *Social Science Research,* 53, pp. 118-136.

Yu, X., and Khazanchi, D. (2019). Using Embedded Mixed Methods in Studying IS Phenomena: Risks and Practical Remedies with an Illustration. *Communications of the Association for Information Systems*, 41, pp. 555-595.

Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviours among young adolescents. *Journal of Consumer Affairs*, 43 (3), pp. 389-418.

Yunus, N., and Rashid, W. (2016). The Influence of Country-of-origin on Consumer Purchase intention: The Mobile Phones Brand from China. *The 5th International Conference on Marketing and Retailing. Procedia Economics and Finance,* 37, pp. 343-349.

Zack, E., Kennedy, J., and Long, J. (2019). Can nonprobability samples be used for social science research? A cautionary tale. Survey Research Methods, 13(1), pp. 215-227.

Zadek, S. (2004). The path to corporate responsibility. *Harvard Business Review*, 82(12), pp. 125-132.

Zellman, G. (1990). Report decision making patterns among mandated child abuse reports. *Child Abuse and Neglect,* 14(3), pp. 325-336.

Zhang, Q., and Ahmad, S. (2021). Analysis of Corporate Social Responsibility Execution Effects on Purchase Intention with the Moderating Role of Customer Awareness. Sustainability, 13, pp. 4548- 4590.

Zhang, R., Chen, J., and Lee, C. (2013). Mobile commerce and consumer privacy concerns. *Journal of Computer Information Systems,* 53(4), pp. 31-38.

Zhou, T. (2015). The effect of perceived justice on LBS users' privacy concern. *Information Development,* 32(5), pp. 1730–1740.

Zuboff, S. (2019). Surveillance Capitalism and the Challenge of Collective Action. *New Labor Forum,* 28(1), pp. 10–29.

Zukowski, T., and Brown, I. (2007). Examining the influence of demographic factors on internet users' information privacy concerns. *Proceedings of the 2007 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries*.

APPENDICES

Appendix A. Study One: Ethical Approval

Ollscoil Chathair Bhaile Átha Cliath
Dublin City University

Ms Valerie Lyons
Dublin City University Business School

10th May 2019

REC Reference: **DCUREC/2019/068**

Proposal Title: **Privacy as a Corporate Social Responsibility**

Applicant(s): **Ms Valerie Lyons**

Dear Valerie,

This research proposal qualifies under our Notification Procedure, as a low risk social research project. Therefore, the DCU Research Ethics Committee approves this project.

Materials used to recruit participants should state that ethical approval for this project has been obtained from the Dublin City University Research Ethics Committee.

Should substantial modifications to the research protocol be required at a later stage, a further amendment submission should be made to the REC.

Yours sincerely,

DCU Research & Innovation

Dr Mark Philbin
Interim Chairperson
DCU Research Ethics Committee

Taighde & Nuálaíocht Tacaíocht
Ollscoil Chathair Bhaile Átha Cliath,
Baile Átha Cliath, Éire

Research & Innovation Support
Dublin City University,
Dublin 9, Ireland

T +353 1 700 8000
F +353 1 700 8002
E research@dcu.ie
www.dcu.ie

Appendix B. Study One: Online Delphi Survey - Round 1 - Invitation

Dear Participant

Thank you for agreeing to participate in our survey. Our research aims to construct a framework for measuring an organisation's privacy orientation. We want to use that framework to position privacy behaviours reported by organisations as either control or justice. To ensure the validity and robustness of the qualitative methodologies used in the study, we would like to leverage the collective knowledge of a panel of experts to agree and categorise a comprehensive list of privacy behaviours as control behaviours or justice behaviours (in the first survey), and to rank how strongly those behaviours demonstrate either control or justice (in the second survey).

Study Method
Please read the following link :privacy survey instructions and narrative. In this link we describe the relationship between control/justice and privacy. The narrative will help you position privacy behaviours outlined in the survey as control behaviours or justice behaviours. You are invited to respond to the surveys across two rounds of interaction. The survey rounds will be carried out online, with information provided and consent obtained before proceeding to the survey component. Withdrawal from this project will not be possible once you have submitted the online survey because the information provided by you will be anonymous and consequently unidentifiable. If you agree to participate in this study, you will need to complete and submit the online survey within two weeks of receiving the invitation email. A reminder email will be sent to you five days before the first survey closes. Each survey round takes approximately fifteen minutes to complete.
The first survey can be accessed at the following link: ${l://SurveyLink?d=Take the Survey}
Or you can copy/paste the URL below into your internet browser: ${l://SurveyURL}

Risks And Benefits Of The Research
There are no direct benefits to the participants. However participants are free to promote their participation once the survey is completed. As the survey is anonymous, there are minimal risks to participants and/or their organisation).

Research Findings
The project outcomes will be used to contribute to a PhD publication which will be submitted to peer-reviewed academic journals for publication and may also be presented at various conferences. The data collected in the survey will be used to 1) improve the validity and credibility of the qualitative methodologies used in the research and 2) to help build a framework that can measure levels of control and justice from organisations' reported privacy behaviours.

Confidentiality And Data Protection
Participation in this study is voluntary, and confidentiality will be maintained. Your decision to participate or not participate in this research will not affect your relationship with DCU or any of the researchers. All responses are anonymous to other participants and are stored on DCU's protected Google Drive. The panel members are not told who other panel members are. Only the participant's email address and name are stored, and survey responses. Although confidentiality is protected and information is anonymous to other participants, legislation such as the criminal justice acts may necessitate the provision of information.

Funding

This PhD is funded by the Irish Research Council and The Irish Institute of Digital Business. The student researcher, Valerie Lyons is a scholarship holder through the Irish Research Council. The supervisors (Prof Theo Lynn and Dr. Lisa van der Werff) are employed by Dublin City University.

Ethics Approval

This research was approved by Dublin City University's Ethics Committee in June 2019. If participants have concerns about this study and wish to contact an independent person, please contact: The Secretary, Dublin City University Research Ethics Committee, c/o Research and Innovation Support, Dublin City University, Dublin 9.Telephone 01-7008000

Thank you for your time.

Valerie Lyons

Appendix C. Study One: Online Delphi Survey – Round 1 - Narrative And Instructions

How To Complete The Survey

To help complete the survey, please first read the following narrative, and then consider if an organisation's privacy behaviours (as outlined in the survey) demonstrate control or justice?

Additionally, If you feel there is a privacy behaviour or activity you feel is commonly reported or published by organisations and is not included here, please outline it in the final section and outline whether you believe it to be a control or justice behaviour.

Narrative: Privacy As Control Or Justice

While there is no single concept of information privacy that crosses all disciplines 'control over personal information' is a common theme across many privacy studies. The definition of privacy offered by Belanger et al. (2002) emphasises the role of controls implemented to restrict the use of personal data. However, privacy is not solely about control but also about information being authorised to flow to specific agents at specific times (Moor, 1997). Moor (1997) argues that in a highly digital culture it is simply not possible to control all personal information. Therefore, he argues, the best way to protect privacy is to ensure the right people have access to relevant information at the right time, giving individuals as much control over personal data as realistically possible (labelling his theory the "control/restricted access" theory of privacy). With ever-increasing complex organisational networks however, such individual control is not realistically possible.

Control can also describe the technologies and processes used to enable privacy protection. Control over privacy is facilitated by the consumer (through 'privacy controls' such as preference management tools, privacy enhancing tools (PETs) or consent etc.) or by the organisation (through 'privacy controls' such as preference manager applications, network access controls, authorisation and authentication controls, privileged identity management tools etc.). Therefore we are presented with two distinct but linked uses of the term control; the consumers control of how their data is processed and the organisations control of that information; and the 'controls' that both the organisation and consumer apply to facilitate protection of the data. Providing the consumer with control over their data can result in an organisation not being able to maximise data use or require the implementation of costly technical tools. An organisation's need to dominate control over data is enshrined in the concept of information ownership, and it is this concept of

control that we apply in our research. Information ownership refers to both the possession of, and responsibility for, information and implies control over that information.

Organisations can re-balance the control-equilibrium by returning a level of control to the consumer. This relinquishing of control is enshrined in the concept of information stewardship. Information stewardship implies that no matter what an organisation does with its consumer's information (for example, selling it to third parties) the organisation always remains responsible and retains oversight of the processing of that information. Consumers who are offered Fair Information Privacy Practices (transparency, preference, purpose, minimisation, limitation, quality, integrity, security, and accountability) have been found to experience increased trust in organisations and FIPPs have been linked to procedural justice (Culnan and Bies, 2003).

In simple terms, as researchers, we view 'control' as organisational power over information, and 'justice' as the re-balance of power between consumer and organisation over information.

Appendix D. Study One: Online Delphi Survey - Round 1 – Survey

Welcome to our survey aimed at categorising privacy behaviours as control-based or justice based behaviours, and thank you for your participation in our survey. This survey takes approximately 15 minutes to complete. There are 6 questions in total, each with a choice of three responses.

If you have not already done so, please read the survey instructions, together with the narrative explaining control and justice. In summary, we interpret 'control' to mean organisational power over consumer information, and 'justice' to mean the re-balance of power between consumer and organisation over consumer information.

Please consent to participate in the survey, by ticking all boxes.

- I have read and understood the survey instructions and narrative☐
- I freely agree to participate in this project according to the conditions in the survey instructions ☐
- I understand the researcher has agreed not to reveal my identity to other participants or at any conferences☐

INFORMATION CUSTODY

Information custody is a term referring to how organisations view rights over customer data. Organisations who view their custody of customer information as 'Steward', consider the customer to be the information owner, whilst still retaining oversight of the processing of information (even when selling it to third parties). Organisations who view their custody of customer information as 'Owner', consider themselves to be the information owner, and may for instance, share information with third parties without the need for oversight. If an organisation demonstrates any of the following behaviours, with regard to information custody, do you feel it would demonstrate values of control or values of justice?

	Control	**Justice**	**Neither**
Ownership of customer information is shared between customer and organisation.	☐	☐	☐
The organisation operates as the owner of customer information	☐	☐	☐
The organisation operates as a steward of customer information	☐	☐	☐

If you selected 'neither' for any option above, can you provide a brief explanation?

PRIVACY CULTURE

If an organisation demonstrates any of the following behaviours, with regard to their privacy culture, do you feel it demonstrates values of control or values of justice?

	Control	Justice	Neither
Organisation publishes their values towards privacy in corporate publications (e.g. reports, websites, policies or other publications/notices)	☐	☐	☐
Organisation does not publish their values towards privacy in corporate publications (e.g. reports, websites, policies or other publications/notices)	☐	☐	☐
Organisation associates privacy with their brand in corporate publications (e.g. reports, websites, policies or other publications/notices)	☐	☐	☐
Organisation exceeds privacy minimums (as mandated by regulations)	☐	☐	☐
Organisation has appointed a privacy representative to the C-Suite (e.g. a chief privacy officer)	☐	☐	☐
Organisation has appointed privacy representatives to management level e.g., a data protection manager	☐	☐	☐

If you selected 'neither' for any option above, can you provide a brief explanation?

ORGANISATIONAL USE OF INFORMATION

If an organisation demonstrates the following behaviours with regard to it's strategic focus and use of customer information, do you feel it demonstrates values of control or values of justice?

	Control	Justice	Neither
Organisation is transaction-focused (aiming to deliver the product for a price)	☐	☐	☐
Organisation is data-focused (aiming to extract data from the customer)	☐	☐	☐
Organisation is inference-focused (aiming to profile customer e.g., for personalisation of adverts)	☐	☐	☐
Organisation is advice-focused (aiming to build relationships with customer)	☐	☐	☐

If you selected 'neither' for any option above, can you provide a brief explanation?

PRIVACY MOTIVATIONS

If an organisation publishes any of the following behaviours in their corporate publications (such as annual reports, privacy policies or corporate social responsibility reports), regarding their motivation towards addressing privacy, do you feel it demonstrates values of control or values of justice?

	Control	Justice	Neither
An organisation's privacy behaviours are driven by consumer trust	☐	☐	☐
An organisation's privacy behaviours are driven by compliance	☐	☐	☐
An organisation's privacy behaviours are driven by a code of ethics	☐	☐	☐
An organisation's privacy behaviours are driven by consumer respect	☐	☐	☐
An organisation's privacy behaviours are driven by consumer loyalty	☐	☐	☐
An organisation's privacy behaviours are driven by Fair Information Privacy Practices (FIPPs)	☐	☐	☐
An organisation's privacy behaviours are aimed at external stakeholders (e.g. customers)	☐	☐	☐
An organisation's privacy behaviours are aimed at internal stakeholders (e.g. employees)	☐	☐	☐
An organisation's privacy behaviours are aimed at stakeholder engagement	☐	☐	☐
An organisation's privacy behaviours are aimed at stockholder/share value	☐	☐	☐

If you selected 'neither' for any option above, can you provide a brief explanation?

PRIVACY BEYOND REGULATION

If an organisation demonstrates any of the following behaviours, with regard to their privacy behaviours that exceed regulation, do you feel it demonstrates values of control or values of justice?

	Control	Justice	Neither
Chequebook privacy(writing a cheque for an event or group, but not being involved)	☐	☐	☐
Participating in public debates on privacy	☐	☐	☐
Advising public policy on privacy	☐	☐	☐
Strategic collaboration with privacy advocacy groups	☐	☐	☐
Sponsoring privacy conferences	☐	☐	☐
Developing open standards for privacy	☐	☐	☐
Privacy related employee training that exceeds regulatory minimum (as per data	☐	☐	☐

protection legislation)			
Lobbying governments for privacy standards that are more beneficial to the organisation than to the customer	☐	☐	☐
Lobbying governments for privacy standards that are more beneficial to the customer than to the organisation	☐	☐	☐
Lobbying governments for privacy standards that are more beneficial to society than to the organisation	☐	☐	☐

If you selected 'neither' for any option above, can you provide a brief explanation?

PRIVACY RESOURCE INVESTMENTS

If an organisation demonstrates any of the following behaviours (with regard to privacy resources) do you feel it demonstrates values of control or values of justice.

	Control	**Justice**	**Neither**
Limited staff assigned to privacy activities	☐	☐	☐
Limited budget assigned to privacy activities	☐	☐	☐
Maximised staff assigned to privacy activities	☐	☐	☐
Maximised staff assigned to privacy activities	☐	☐	☐
Maximised budget assigned to privacy activities	☐	☐	☐
An organisation's customers are not privacy aware	☐	☐	☐
An organisation's customers value privacy and monitor/manage their privacy	☐	☐	☐
An organisation links privacy to the customer	☐	☐	☐

If you selected 'neither' for any option above, can you provide a brief explanation?

THANK YOU FOR YOUR PARTICIPATION

Thank you for your participation, your time and your contribution. Please feel free to list any other organisational privacy behaviours not included above, and classify as a control or justice behaviour:

Appendix E. Study One: Online Delphi Survey - Reminder Emails

Dear Participant

Thank you for agreeing to participate in our survey. We are coming to the end of week 1 of Survey No.1. It would be much appreciated if you could complete Survey No.1 before week ending Friday 28th of June. This will allow us to collect the data and compose Survey No.2. The 2nd survey is aimed at simply ranking the behaviours agreed in the Survey No.1.

Follow this link to Survey No.1:
${l://SurveyLink?d=Take the Survey}

Or copy and paste the URL below into your internet browser:
${l://SurveyURL}

Many thanks in advance for your participation.

Regards

Valerie Lyons

Follow the link to opt out of future emails:
${l://OptOutLink?d=Click here to unsubscribe}

Dear Survey Participants,

Many thanks to those of you who have completed the survey already. Survey No.1 closes tomorrow so it would be much appreciated if you can complete Survey No.1 if you have not done so already. Results from Survey No.1 will be compiled into Survey No.2 and redistributed next week.

If you do not wish to participate, it would be much appreciated if you can click on the opt out button below.

Again, many thanks for your participation.

Regards

Appendix F. Study One: Online Delphi Survey - Round 2 Survey

Dear Participant,

Thank you for your participation in this exercise and welcome to the final round of our survey. This round is aimed at ranking levels of control or justice demonstrated by privacy behaviours which were analysed in survey round No.1, and takes approximately 20 minutes to complete.

The survey is divided into three sections. The first section lists the privacy behaviours that were favoured by participants as Control, followed by the privacy behaviours favoured as Justice. Based on feedback from respondents - 'neither' was interpreted by participants in survey No.1 to mean 'neither' or 'both'. Therefore where results favoured a behaviour as 'neither' in survey No.1, the behaviour has been moved to the third and final section of survey No.2, to be categorised as neither, or both.

IMPORTANT NOTE: The position of a particular behaviour may not be unanimously supported by all participants. This is the purpose of using a large panel of global experts. If you do not agree with the statistical positioning, then do not complete that particular item, and we will interpret your non-response as 'I do not agree with the position'. However before doing that please read the following important clarification : In this exercise we ask that you consider only 'the values being demonstrated' by a privacy behaviour, rather than considering the underpinning motivations or interpretations of an organisation in undertaking that behaviour. By way of example, an organisation participating in lobbying for enhanced consumer privacy might be considered to demonstrate values of justice. If we were to consider the organisation's strategic agenda for undertaking such a privacy behaviour - we might hypothesize that an organisation who sells a privacy-enhancing-technology would benefit from such a behaviour and that it could therefore demonstrate either control or justice. However for the purpose of this survey, we are evaluating behaviours 'at face value' and not trying to 'second guess' the reasons an organisation might undertake particular behaviours.

To recap on our interpretation of control and justice, please re-read the narrative explaining the relationship between control and justice in the context of privacy. In summary, we interpret 'control' to mean organisational power over consumer information, and 'justice' to mean the rebalance of power between consumer and organisation over consumer information.

CONSENT

Please consent to participate in the survey, by ticking all boxes.

- I have read and understood the survey instructions and narrative ☐
- I freely agree to participate in this project according to the conditions in the survey instructions ☐
- I understand the researcher has agreed not to reveal my identity to other participants, or at any conferences ☐

THE FOLLOWING SECTIONS LISTS THE CONTROL BEHAVIOURS, AS FAVOURED BY PARTICIPANTS IN ROUND No.1

INFORMATION CUSTODY - CONTROL

How much CONTROL do you feel these behaviours demonstrate on a scale ranging from low to high?

	1 Low-	2 Low-Moderate	3 Moderate	4 Moderate-High	5 High
The organisation operates as the owner of customer information (reminder: organisations who view their custody of customer information as 'Owner', consider themselves to be the information owner, and may for instance, share information with third parties without the need for oversight).	□	□	□	□	□
Ownership of customer information is shared between customer and organisation, however the organisation dominates ownership	□	□	□	□	□
Organisation is transaction-focused (aiming to deliver the product for a price)	□	□	□	□	□
Organisation is data- focused (aiming to extract data from the customer)	□	□	□	□	□
Organisation is inference-focused (aiming to profile customer e.g., for personalisation of adverts)	□	□	□	□	□

PRIVACY MOTIVATIONS - CONTROL

If an organisation publishes any of the following behaviours in their corporate publications (such as annual reports, privacy policies or corporate social responsibility reports), regarding their motivation towards addressing privacy, how much CONTROL do you feel these behaviours demonstrate on a scale ranging from low to high?

	1 Low-	2 Low-Moderate	3 Moderate	4 Moderate-High	5 High
An organisation's privacy behaviours are aimed at external stakeholders (e.g. customers)	□	□	□	□	□
An organisation's privacy behaviours are aimed at stockholder/share value	□	□	□	□	□
Organisation does not publish their values towards privacy in corporate publications (e.g. reports, websites, policies or other publications/notices)	□	□	□	□	□

PRIVACY BEYOND REGULATION - CONTROL

If an organisation demonstrates any of the following behaviours, with regard to their privacy behaviours that exceed regulation, how much CONTROL do you feel these behaviours demonstrate on a scale ranging from low to high?

	1 Low-	2 Low-Moderate	3 Moderate	4 Moderate-High	5 High
Chequebook privacy (writing a cheque for a privacy event or group, but not being involved)	☐	☐	☐	☐	☐
Lobbying governments for privacy standards that are more beneficial to the organisation than to the customer	☐	☐	☐	☐	☐

PRIVACY RESOURCE INVESTMENTS-CONTROL

If an organisation demonstrates any of the following behaviours (with regard to privacy resources) how much CONTROL do you feel these behaviours demonstrate on a scale ranging from low to high control ?

	1 Low-	2 Low-Moderate	3 Moderate	4 Moderate-High	5 High
Limited staff assigned to privacy activities	☐	☐	☐	☐	☐
Limited budget assigned to privacy activities	☐	☐	☐	☐	☐
An organisation's customers are not privacy aware	☐	☐	☐	☐	☐

THE FOLLOWING SECTIONS LISTS THE JUSTICE BEHAVIOURS, AS FAVOURED BY PARTICIPANTS IN ROUND No.1

INFORMATION CUSTODY AND USE – JUSTICE

If an organisation demonstrates any of the following behaviours (with regard to information custody and information use), how much JUSTICE do you feel these behaviours demonstrate on a scale ranging from low to high?

	1 Low-	2 Low-Moderate	3 Moderate	4 Moderate-High	5 High
The organisation operates as a steward of customer information (reminder: organisations who view their custody of customer information as 'Steward' may for instance, share information with third parties whilst still retaining oversight of that data).	□	□	□	□	□
The organisation operates as a steward of customer information (reminder: organisations who view their custody of customer information as 'Steward' may for instance, share information with third parties whilst still retaining oversight of that data).	□	□	□	□	□
Ownership of customer information is shared between customer and organisation, however the customer dominates ownership	□	□	□	□	□
Organisation is advice-focused (aiming to build relationships with customer	□	□	□	□	□

PRIVACY RESOURCES - JUSTICE

How much JUSTICE do you feel these privacy culture behaviours demonstrate on a scale ranging from low to high?

	1 Low-	2 Low-Moderate	3 Moderate	4 Moderate-High	5 High
Maximised staff assigned to privacy activities	□	□	□	□	□
Maximised budget assigned to privacy activities	□	□	□	□	□
An organisation's customers value privacy and monitor/manage their privacy	□	□	□	□	□
An organisation links privacy to the customer	□	□	□	□	□

PRIVACY MOTIVATIONS AND CULTURE – JUSTICE

How much JUSTICE do you feel these privacy culture behaviours demonstrate on a scale ranging from low to high?

	1 Low-	2 Low-Moderate	3 Moderate	4 Moderate-High	5 High
Organisation publishes their values towards privacy in corporate publications (e.g. reports, websites, policies etc)	□	□	□	□	□
Organisation exceeds regulated or legislative privacy minimums	□	□	□	□	□
Organisation has appointed a privacy representative to the C-Suite (e.g. a chief privacy officer)	□	□	□	□	□
Organisation has appointed privacy representatives to management level e.g., a data protection manager	□	□	□	□	□
An organisation's privacy behaviours are driven by consumer trust	□	□	□	□	□
An organisation's privacy behaviours are driven by a code of ethics	□	□	□	□	□
An organisation's privacy behaviours are driven by consumer respect	□	□	□	□	□
An organisation's privacy behaviours are driven by consumer loyalty	□	□	□	□	□
An organisation's privacy behaviours are driven by Fair Information Privacy Practices (FIPPs)	□	□	□	□	□

PRIVACY EXCEEDING REGULATION - JUSTICE

How much JUSTICE do you feel these privacy culture behaviours demonstrate on a scale ranging from low to high?

	1 Low-	2 Low-Moderate	3 Moderate	4 Moderate-High	5 High
Organisation engages in strategic collaborations with privacy advocacy groups	□	□	□	□	□
Organisation develops open standards for privacy	□	□	□	□	□
Organisation provides privacy related training to employees that exceeds regulatory minimum	□	□	□	□	□
Organisation lobbies governments for privacy standards that are more beneficial to the customer than to the organisation	□	□	□	□	□
Organisation lobbies governments for privacy standards that are more beneficial to society than to the organisation	□	□	□	□	□

THE FOLLOWING SECTION LISTS THE 'NEITHER' BEHAVIOURS (AS FAVOURED BY PARTICIPANTS IN ROUND No.1)

In Survey No.1 comments and feedback, many of you interpreted 'neither' to mean 'neither' or 'both', as the option for 'both' was not available. To address this concern, it would be much appreciated if you could indicate whether you consider the following behaviours as 'neither', or both (control is greater) or both (justice is greater) or both (equal). We appreciate you may not have chosen these behaviours as 'neither' and if so, there is no need to respond to any you disagree with.

	Neither **Neither Control nor Justice are demonstrated**	**Both** **More Control demonstrated than Justice**	**Both** **More Justice demonstrated than Control**	**Both** **Control and Justice are equally balanced**
An organisation has appointed privacy representatives that are low profile nonexecutive management	☐	☐	☐	☐
An organisation associates privacy with their brand in corporate publications (e.g. reports, websites, policies or other publications/notices)	☐	☐	☐	☐
An organisation's privacy behaviours are aimed at internal stakeholders	☐	☐	☐	☐
An organisation's privacy behaviours are aimed at external stakeholders	☐	☐	☐	☐
An organisation's privacy behaviours are driven by compliance	☐	☐	☐	☐
An organisation sponsors privacy conferences	☐	☐	☐	☐
An organisation participates in public debates on privacy	☐	☐	☐	☐
An organisation advises public policy on privacy	☐	☐	☐	☐
An organisation has limited staff assigned to privacy activities	☐	☐	☐	☐

THANK YOU FOR YOUR PARTICIPATION

Thank you for your participation, your time and your contribution. Please feel free to list any other organisational privacy behaviours not included above, and classify as a control or justice behaviour:

Appendix G. Study One: Totals from Both Rounds

	NMPv Activity	*Round 1*	*Round 2 (Part I) - Weight*	*Round 2 (Part II) - Clarification And Ambiguity*
			Weight (Median)	
1	***SharedOwnOrgMore***	Control	4	
2	***Owner***	Control	5	
3	***InfoSteward***	Justice	4	
4	***PubValue***	Justice	4	
5	***NoPubValue***	Control	3.5	
6	***PrivLink2Brand***	Justice	1	More Justice than Control
7	***ExceedPrivMin***	Justice	5	
8	***Csuite***	Justice	4.5	
9	***Dpo***	Justice	4	
10	***Transfocus***	Control	3	
11	***DataFocus***	Control	5	
12	***InferFocus***	Control	5	
13	***AdviceFocus***	Justice	4	
14	***DrivnByConTrust***	Justice	4.5	
15	***DrivnByCompliance***	Control	1	More Control than Justice
16	***DrivnByEthic***	Justice	4	
17	***DrivnByConRespect***	Justice	4	
18	***DrivnByConsLoyal***	Justice	3.5	
19	***DrivnFIPPS***	Justice	3.5	
20	***DrivByStock/ShareValue***	Control	4	
21	***Aimed@ext***	Control	1	More Control than Justice
22	***Aimed@int***	Control	1	More Control than Justice
23	***PubDebates***	Justice	1	More Justice than Control
24	***AdvisePubPol***	Justice	1	More Justice than Control
25	***StratCollab***	Justice	5	
26	***SponsorLinkConf***	Justice	1	More Justice than Control
27	***DevOpnStds***	Justice	4	
28	***EmpTrainExceed***	Justice	4	
29	***LobbyOrg***	Control	4	
30	***LobbyCons***	Justice	4	
31	***LobbySoc***	Justice	5	
32	***LtdStaff***	Control	3	*1*
33	***LtdBudget***	Control	3	
34	***MaxStaff***	Justice	4	
35	***MaxBudgt***	Justice	4	
36	***CustNotPrivAware***	Control	3	
37	***CustValuePriv***	Justice	5	
38	***OrgLinksPrivtoCus***	Justice	5	
39	***LowProfNonExec***	Control	1	More Control than Justice
40	***SharedOwnerIndivMore***	Justice	1	More Justice than Control

Appendix H. Study One: Organisations by Industry

Aerospace and	Chemicals	Energy	Finance	Food & Drug	Food, Beverages & Tobacco	Healthcare	Industrials	Media	Motor Vehicles	Oil & Gas Equip	Retail	Tech	Telecom	Transport	Wholesalers
3	3	10	21	2	6	15	4	2	2	2	8	10	4	5	3
Boeing	3M	Chevron	AIG	Kroger	Archer Daniels Midland	Express Scripts	Caterpillar	Walt Disney	Ford Motor	Enterprise Products	Amazon	Alphabet	AT&T	American Airlines	Sysco
General Dynamics	Dow	Conoco Phillips	Allstate	Walgreens Boots	CHS	Procter & Gamble	Deere	21st Cent Fox WaltDisney	General Motors	Halliburton	Best Buy	Apple	Comcast	Delta Air Lines	Ingram
Lockheed Martin	Dupont	Energy Transfer	American Express		Coca-Cola	Aetna	General Electric				Costco	Cisco	Verizon	FedEx	TechData
		Phillips 66	Bank of America		Mondelez	Amerisource Bergen	Honeywell				Home Depot	Dell	DirectTv-AT&T	United Airlines	
		Exxon Mobile	Berkshire Hathaway		PepsiCo	Anthem					Lowe's	Facebook		United Parcel	
		Plains GP Holdings	Citi		Tyson Foods	Cardinal Health					Macy /Sears	HP			
		Valero Energy	Fannie Mae			Cigna					Target	IBM			
		World Fuel	Freddie Mac			CVS Health					Walmart	Intel			
		Andeavor (by/Marathon)	Goldman Sachs			HCA Healthcare						Microsoft			
		Marathon Petroleum	JP Morgan			Humana						Oracle			
			Liberty Mutual			Johnson & Johnson									
			Mass Mutual			McKesson									
			MetLife			Merck									
			Morgan Stanley			Pfizer									
			Nation wide			United Health									
			NewYork life												
			Prudntial Financial												
			State Farm												
			StoneX												
			TIAA												
			Wells Fargo												

Appendix I. Study One: NMPv Orientations of the Organisations

Risk Management	**Integrated**	**Warrior**	**Citizenship**
n=55	*n*=2	*n*=6	*n*=2
3M	Best Buy	Allstate	AT&T
Aetna	General Motors	Apple	Verizon
AIG		Cisco	
Alphabet		HP	
Amazon		IBM	
American Airlines		Microsoft	
American Express			
Amerisource Bergen			
Anthem			
Cardinal			
Chevron			
Cigna			
Citigroup			
Conoco			
CVS			
Deere			
Dell			
Delta			
Dupont			
Enterprise			
FedEx			
Ford Motor			
General Dynamics			
General Electric			
Goldman Sachs			
Home Depot			
Honeywell			
Humana			
Ingram			
Intel			
J&J			
Kroger			
Liberty			
Lockheed			
Lowe's			
Macy /Sears			
Marathon			
Merck			
MetLife			
Morgan Stanley			
Nationwide			
Oracle			
Pfizer			
P&G			
Prudential			
Target			
TechData			
TIAA			
UPS			
United Health			
Valero			
Walmart			
Walt Disney			
Wells Fargo			
World Fuel			

Appendix J. Study One: Organisations listed in the Forbes 100 JUST companies and Fortune 100.

Company Name	Industry	Just 100
Lockheed Martin	Aerospace & Defence	JUST 53
3M	Chemicals	JUST 90
Chevron	Energy	JUST 61
Marathon	Energy	JUST 79
MetLife	Financials (insurance)	JUST 75
Bank of America	Financials (banking)	JUST 12
Citigroup	Financials (banking)	JUST 31
JPMorgan Chase	Financials (banking)	JUST 6
Wells Fargo	Financials (banking)	JUST 72
American Express	Financials (banking)	JUST 89
PepsiCo	Food, Beverages & Tobacco	JUST 24
Coca-Cola	Food, Beverages & Tobacco	JUST 95
Merck	Healthcare (drugs)	JUST 30
Cigna	Healthcare (insurance)	JUST 17
Humana	Healthcare (insurance)	JUST 52
Anthem	Healthcare (retail)	JUST 14
CVS Health	Healthcare (retail)	JUST 84
Procter & Gamble	Healthcare (wholesale)	JUST 18
Johnson & Johnson	Healthcare (wholesale)	JUST 45
Deere	Industrials	JUST 70
General Motors	Motor Vehicles & Parts	JUST 28
Ford Motor	Motor Vehicles & Parts	JUST 37
Target	Retailing	JUST 15
Best Buy	Retailing	JUST 25
Walmart	Retailing	JUST 50
Amazon	Retailing	JUST 66
Home Depot	Retailing	JUST 84
IBM	Technology	JUST 11
HP	Technology	JUST 16
Apple	Technology	JUST 3
Dell	Technology	JUST 35
Intel	Technology	JUST 4
Alphabet	Technology	JUST 5
Cisco Systems	Technology	JUST 9
Microsoft	Technology	JUST 1
Verizon	Telecommunications	JUST 42
Comcast	Telecommunications	JUST 49
AT&T	Telecommunications	JUST 8
UPS	Transportation	JUST 39
FedEx	Transportation	JUST 82
Delta Air Lines	Transportation	JUST 97

Appendix K. Study Two: Experimental Vignette Survey (Experiment 1) - Ethical Approval

Ollscoil Chathair Bhaile Átha Cliath
Dublin City University

DCU

Ms Valerie Lyons
Dublin City University Business School

2nd August 2019

REC Reference: DCUREC/2019/133

Proposal Title: Corporate Political Privacy

Applicant(s): Ms Valerie Lyons, Prof. Theo Lynn and Dr Lisa Van Der Werff

Dear Colleagues,

This research proposal qualifies under our Notification Procedure, as a low risk social research project. Therefore, the DCU Research Ethics Committee approves this project.

Materials used to recruit participants should state that ethical approval for this project has been obtained from the Dublin City University Research Ethics Committee.

Should substantial modifications to the research protocol be required at a later stage, a further amendment submission should be made to the REC.

Yours sincerely,

DCU
Research & Innovation

Dr Mark Philbin
Interim Chairperson
DCU Research Ethics Committee

Taighde & Nuálaíocht Tacaíocht
Oifigeil Chathair Bhaile Átha Cliath
Baile Átha Cliath, Éire

Research & Innovation Support
Dublin City University
Dublin 9, Ireland

T +353 1 700 8000
F +353 1 700 8002
E research@dcu.ie
www.dcu.ie

Appendix L. Study Two: Experimental Vignette Survey (Experiment 1) - Survey

Dear Participant,

Thank you for participating in this survey. This survey aims to research the potential impact that organisations' responses to privacy can have on stakeholders.

In the first part of this survey – you will be asked a series of questions about your attitudes to both privacy and trust. You will then be provided with a randomly selected scenario, outlining the privacy activity of a fictitious organisation called 'ModernTech'. You will be asked a final series of questions regarding your attitudes towards ModernTech. The survey should take between 7-10 minutes to complete and requires that you are over 18 years of age. A small number of questions in the survey require a correct answer, and if failed will route the participant to the end of the survey without a completion code. If you agree to participate in this survey, you will need to complete and submit the online survey within two weeks of starting. A reminder email will be sent to you five days before the survey close date.

Confidentiality and Data Protection

Participation in this study is voluntary, and confidentiality will be maintained. Your decision to participate or not participate in this research will not affect your relationship with DCU or any of the researchers. All responses are anonymous and are stored on DCU's protected Google Drive. Although confidentiality is protected, and information is anonymous, legislation such as the criminal justice acts may necessitate the provision of information.

If participants have concerns about this study and wish to contact an independent person, please contact: The Secretary, Dublin City University Research Ethics
Committee, c/o Research and Innovation Support, Dublin
City University, Dublin 9. Tel 01-7008000

Thank you for your time.

Consent Section

- I have read & understand the Plain Language Statement providing details of the survey □
- I freely agree to participate in this project according to the conditions in the Plain Language Statement□
- I am aware that this survey is anonymous and that my personal details will not be processed, published or presented in any public form. □
- I am over 18 years of age□

Control /DVs Section

What is your Worker ID in Mechanical Turk?

Q1. What is your age?

18-20 □

21-25 □

26-30 □

31-35 □

36-40 □

41-45 □

46-50 □

51-55 □

56-60 □

61-65□

66 Plus □

Q2. What country are you from?

Q3. What is your sex?

Male □

Female □

Prefer not to say□

Q5. For each of the following statements, please outline how much you agree with the statement on a scale of 1-5, where 1 is strongly disagree and 5 is strongly agree.

	1 Strongly disagree	2 Somewhat disagree	3 Neither agree nor disagree	4 Somewhat agree	5 Strongly agree
My tendency to trust other is high	□	□	□	□	□
My typical approach is to trust new acquaintances until they prove I should not trust them	□	□	□	□	□
Trusting another person is not difficult for me	□	□	□	□	□
I usually trust people until they give me a reason not to trust them	□	□	□	□	□
Compared to others, I am more sensitive about the way companies handle my personal information	□	□	□	□	□
To me, it is the most important thing to keep my information private.	□	□	□	□	□
Compared toothers, I tend to be more concerned about threats to my information privacy	□	□	□	□	□

Experiment Section

The following passage describes a fictitious organisation that we would like you to imagine you are a customer of. Please read this passage carefully along with the statement on the next page.

"ModernTech is a (fictitious) large North American technology organization, providing online services/products to 50 million customers. ModernTech has to process certain consumer data in order to complete a transaction (e.g. credit card details, expiry dates and transaction details) or in order to register an account (such as name, date of birth, address, email etc). Imagine that you recently purchased a repeating monthly subscription to use one of ModernTech's mobile applications and you have disclosed information to ModernTech during this purchase, such as your credit card details, your email address and your mobile phone number".

Please read the above passage carefully. What did you (hypothetically) purchase recently from ModernTech in the above scenario? If the answer to this question is incorrect, the survey will terminate.

Vignettes 01: Moderntech Beneficiary, Consumers Disadvantaged
We would like you to imagine that you read the following information regarding ModernTech: "ModernTech is not supportive of proposals for a new privacy regulation, called The Ultimate Privacy Act, which requires that organisations provide a 'Do Not Sell or Share My Data' option to their consumers. ModernTech objects to these requirements, as they would reduce the amount of data ModernTech can share/sell and would therefore negatively impact their efforts to maximize profit."
OR **Vignettes 02: ModernTech Beneficiary, Individual Disadvantaged**
We would like you to imagine that you read the following information regarding ModernTech: ModernTech is not supportive of proposals for a new privacy regulation, called The Ultimate Privacy Act, which requires that organisations provide a 'Do Not Sell Or Share My Data' option to their consumers. Lawmakers have suggested that these requirements be extended in due course to all individuals in society e.g., taxpayers, website visitors, patients, students etc. ModernTech objects to these requirements, and objects to extending these requirements to all individuals in society, as these proposals would reduce the amount of data that ModernTech can share/sell, and therefore negatively impact their efforts to maximize profit.
OR **Vignettes 03: ModernTech Disadvantaged, Consumer Beneficiary**
We would like you to imagine that you read the following information regarding ModernTech: "ModernTech is supportive of proposals for a new privacy regulation, called The Ultimate Privacy Act, which requires organisations to provide a 'Do Not Sell Or Share My Data' option to their consumers. Although ModernTech accepts that these requirements will reduce the amount of data they can share/sell (and therefore negatively impacts their efforts to maximize profit), ModernTech recognizes the importance of strengthening privacy regulation for consumers".
OR **Vignette 04: ModernTech Disadvantaged, Individuals Beneficiary** *We would like you to imagine that you read the following information regarding ModernTech: "ModernTech is supportive of proposals for a new privacy regulation, called The Ultimate Privacy Act, which requires organisations to provide a 'Do Not Sell Or Share My Data' option to their consumers. Lawmakers have suggested that these requirements be extended in due course to all individuals in society e.g., taxpayers, website visitors, patients, students etc. Although ModernTech accepts that these requirements will reduce the amount of data they can share/sell (and therefore negatively impacts their efforts to maximize profit), ModernTech also recognises the importance of strengthening privacy regulation for society, and therefore supports extending these requirements to all individuals".*

Q6&7. Based on what you have just read about ModernTech, please answer the following question:

Does ModernTech support strengthening data privacy rights for all individuals in society? Y/N

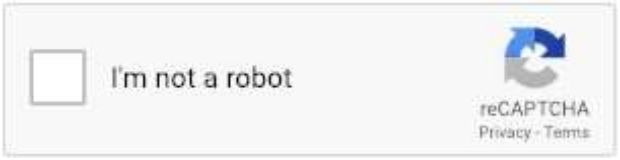
Does ModernTech aims to maximize their opportunity to profit from selling/sharing data? Y/N

Q8. Based on what you have just read about ModernTech, please answer the following questions:

	1 Strongly disagree	2 Somewhat disagree	3 Neither agree nor disagree	4 Somewhat agree	5 Strongly agree
I would be concerned about providing personal information to ModernTech because of what they might do with it that I am unaware of.	□	□	□	□	□
Given the chance, I would be likely to purchase from ModernTech again	□	□	□	□	□
I would be concerned that others can find personal information about me from ModernTech	□	□	□	□	□
It is likely that I would buy products/services from ModernTech in the near future	□	□	□	□	□
I would be concerned that the information I provide to ModernTech could be misused	□	□	□	□	□
ModernTech respects its customers' privacy	□	□	□	□	□
I would be concerned about submitting my personal information to ModernTech because it could be used in a way I did not foresee.	□	□	□	□	□
Given the chance, I predict that I would be likely to purchase from ModernTech in the future.	□	□	□	□	□

Q9. After reading the ModernTech scenario, rate the extent to which you agree with the following (where 1 means strongly disagree and 5 means strongly agree):

	1 Strongly disagree	2 Somewhat disagree	3 Neither agree nor disagree	4 Somewhat agree	5 Strongly agree
ModernTech is a trustworthy organisation	□	□	□	□	□
ModernTech could be relied on to keep its promises to protect the privacy of my personal information	□	□	□	□	□
I could count on ModernTech to protect the privacy of my personal information	□	□	□	□	□
I could count on ModernTech to protect customers' personal information from misuse	□	□	□	□	□



Here is your completion ID : ${e://Field/Random%20ID} _____

When you have copied this ID into Mechanical Turk, please complete your worker id, and click the next button to submit your survey. Thank you for your participation in our study - we really appreciate your contribution. Please feel free to add any comments that may help us improve our survey.

Appendix M. Study Two: Experimental Vignette Survey (Experiment 2) - Ethical Approval

Ollscoil Chathair Bhaile Átha Cliath
Dublin City University

DCU

Ms. Valerie Lyons
DCU Business School

Prof. Theo Lynn
DCU Business School

Dr. Lisa van der Werff
DCU Business School

26th January 2021

REC Reference: **DCUREC/2021/006**

Proposal Title: **An Exploration of Nonmarket Privacy Strategies and Activities.**

Applicant(s): **Ms. Valerie Lyons, Prof. Theo Lynn, and Dr. Lisa van der Werff**

Dear Colleagues,

This research proposal qualifies under our Notification Procedure, as a low risk social research project. Therefore, the DCU Research Ethics Committee approves this project.

Materials used to recruit participants should state that ethical approval for this project has been obtained from the Dublin City University Research Ethics Committee.

Should substantial modifications to the research protocol be required at a later stage, a further amendment submission should be made to the REC.

Yours sincerely,

Geraldine Scanlon

Dr Geraldine Scanlon
Chairperson
DCU Research Ethics Committee

DCU
Research & Innovation

Taighde & Nuálaíocht Tacaíocht
Ollscoil Chathair Bhaile Átha Cliath,
Baile Átha Cliath, Éire

Research & Innovation Support
Dublin City University
Dublin 9, Ireland

T +353 1 700 8000
F +353 1 700 8002
E research@dcu.ie
www.dcu.ie

Appendix N. Study Two: Experimental Vignette Survey (Experiment 2) - Survey

Dear Participant,

Thank you for participating in this survey. This survey aims to research the potential impact that organisations' responses to privacy can have on stakeholders.

In the first part of this survey – you will be asked a series of demographic questions such as age, gender etc. You will then be provided with a randomly selected scenario, outlining the privacy activity of a fictitious organisation called 'ModernTech'. You will be asked a series of questions regarding your attitudes towards ModernTech and then you will be asked a series of questions regarding your own characteristics. All questions in the survey require a response. The survey should take between 8-10 minutes to complete and requires that you are over 18 years of age. A small number of questions in the survey require a correct answer, and if failed will route the participant to the end of the survey without a completion code. If you agree to participate in this survey, you will need to complete and submit the online survey within two weeks of starting. A reminder email will be sent to you five days before the survey close date.

Confidentiality and Data Protection

Participation in this study is voluntary, and confidentiality will be maintained. Your decision to participate or not participate in this research will not affect your relationship with DCU or any of the researchers. All responses are anonymous and are stored on DCU's protected Google Drive. Although confidentiality is protected, and information is anonymous, confidentiality of information can only be protected within the limitations of the law - i.e., it is possible for data to be subject to subpoena, freedom of information claim or mandated reporting by some professions.

If participants have concerns about this study and wish to contact an independent person, please contact: The Secretary, Dublin City University Research Ethics
Committee, c/o Research and Innovation Support, Dublin
City University, Dublin 9. Tel 01-7008000

Thank you for your time.

Consent Section

- I have read, and I understand the Plain Language Statement providing details of the survey. Y/N
- I freely agree to participate in this project according to the conditions in the Plain Language Statement. Y/N
- I am aware that this survey is anonymous and that my personal details will not be processed or presented in any public form. Y/N
- I understand the information in relation to Data Protection and that confidentiality of information is provided subject to legal limitations. Y/N
- I am over 18 years of age. Y/N

Control Variables

What is your Worker ID in Mechanical Turk?

Q1. What is your age?

18-20 □
21-25 □
26-30 □
31-35 □
36-40 □
41-45 □
46-50 □
51-55 □
56-60 □
61-65□
66 Plus □

Q2. What country are you from?

Q3. What is your sex?

Male □

Female □

Prefer not to say□

Q4. Please indicate your occupation:

Management, professional, and related □
Service □
Sales and office□
Farming, fishing, and forestry□
Construction, extraction, and maintenance□
Production, transportation, and material moving□
Government□
Retired□
Unemployed□
Student□
Other□

Experiment Section

The following passage describes a fictitious organisation that we would like you to imagine you are a customer of. Please read this passage carefully along with the statement on the next page.

ModernTech is a hypothetical large North American technology organisation, providing subscription-based email systems to 40 million customers across the United States. Imagine that in 2020, a new law was introduced in the United States, called the Federal Data Surveillance Act. This law, which was introduced to enhance national security and anti-fraud measures, allows government agencies to access personal data on-demand, in organisations such as ModernTech. Imagine that you recently set up and registered to use an email account from ModernTech, and you often use this account to send personal emails such as those to your friends, family, financial institutions, public agencies and health institutions etc.

Q5. Please read the above passage carefully. In the above scenario with ModernTech, what did you (hypothetically) recently set up and register to use ? If the answer to this question is incorrect, the survey will terminate.

Vignettes 01: CSR Moderntech Beneficiary, Consumers Disadvantaged
After hypothetically setting up and using ModernTech's email system, we would like you to imagine that you read the following information regarding ModernTech:
"ModernTech responds to all requests for consumers personal information made by the government under the Federal Data Surveillance Act, as it helps ModernTechs compliance obligations".
OR
Vignettes 02: CSR ModernTech Disadvantaged, Consumer Beneficiary
After (hypothetically) setting up and using your ModernTech email account, we would like you to imagine that you read the following information regarding ModernTech:
"ModernTech refuses to comply with government requests for personal information made under the Federal Data Surveillance Act, as it interferes with the consumer's right to privacy".
OR
Vignettes 03: CPA ModernTech Beneficiary, Consumer Disadvantaged
After (hypothetically) setting up and using your ModernTech email account, we would like you to imagine that you read the following information regarding ModernTech:
"ModernTech lobbies government in support of the requirements of the Federal Data Surveillance Act, as it helps with ModernTech's compliance obligations".
OR
Vignettes 04: CPA ModernTech Disadvantaged, Consumer Beneficiary
After (hypothetically) setting up and using your ModernTech email account, we would like you to imagine that you read the following information regarding ModernTech:
"ModernTech lobbies government against the Federal Data Surveillance Act, as it interferes with the consumer's right to privacy"

Q6. Based on what you have just read about ModernTech, please answer the following question:

The above statement benefits ModernTech (and/or Government) more than the consumer Y/N

Q7. What is the name of the fictitious organisation in the hypothetical scenario above?

- ModernSoft □
- ModernTech □
- TechSoft □

Questions (Q8-Q10) are related specifically to your attitudes towards ModernTech - after reading the hypothetical scenario described earlier.

Q8. After reading the ModernTech scenario, rate the extent to which you agree with the following statements (where 1 means strongly disagree and 5 means strongly agree):

	1 Strongly disagree	**2 Somewhat disagree**	**3 Neither agree nor disagree**	**4 Somewhat agree**	**5 Strongly agree**
I could count on ModernTech to protect customers' personal information from misuse	□	□	□	□	□
I could count on ModernTech to protect the privacy of my personal information	□	□	□	□	□
ModernTech has high moral Standards regarding customers information	□	□	□	□	□
I could trust ModernTech	□	□	□	□	□

Q9. After reading the ModernTech scenario, rate the extent to which you agree with the following statements (where 1 means strongly disagree and 5 means strongly agree):

	1 Strongly disagree	2 Somewhat disagree	3 Neither agree nor disagree	4 Somewhat agree	5 Strongly agree
I believe that email accounts such as ModernTech's are already monitored at least part of the time.	☐	☐	☐	☐	☐
I feel that as a result of my using my ModernTech email account, others know information about me more than I am comfortable with.	☐	☐	☐	☐	☐
I would be concerned about submitting my personal information to ModernTech because it could be used in a way I did not foresee.	☐	☐	☐	☐	☐
I am concerned that organisations and/or goverrnments may monitor activities of my email account	☐	☐	☐	☐	☐
I am concerned that the information I provide to ModernTech could be misused.	☐	☐	☐	☐	☐
I believe that as a result of using my ModernTech email account, information about me that I consider private is now more readily available to others than I would want.	☐	☐	☐	☐	☐
I am concerned that ModerrnTech can collect too much information about me.	☐	☐	☐	☐	☐
I would be concerned that others can find personal information about me from ModernTech	☐	☐	☐	☐	☐
I would be concerned about providing personal information to ModernTech because of what they might do with it that I am unaware of.	☐	☐	☐	☐	☐
I feel that as a result of using my ModernTech email account, information about me is out there that, if used, will invade my privacy.	☐	☐	☐	☐	☐

Q10. After reading the ModernTech scenario, please rate the extent to which you agree with the following (on a scale of 1-5, where 1 is strongly disagree and 5 is strongly agree):

	1 Strongly disagree	**2 Somewhat disagree**	**3 Neither agree nor disagree**	**4 Somewhat agree**	**5 Strongly agree**
I would continue using ModernTech's email system to send emails to my friends, family, doctor and other personal connections.	□	□	□	□	□
I would plan to continue using ModernTech's email system to send emails to my friends, family, doctor and other personal connections as soon as possible.	□	□	□	□	□
My intention would be to continue using ModernTech's email system to send emails to my friends, family, doctor and other personal connections.	□	□	□	□	□

Questions (Q11-Q14) are not related specifically to the ModernTech scenario, but are related more to your own personal characteristics.

Q11. For each of the following statements, please rate the extent to which you agree with the statement (on a scale of 1-5, where 1 is strongly disagree and 5 is strongly agree):

	1 Strongly disagree	2 Somewhat disagree	3 Neither agree nor disagree	4 Somewhat agree	5 Strongly agree
Compared to others, I am more sensitive about the way companies handle my personal information	☐	☐	☐	☐	☐
Compared to others, I tend to be more concerned about threats to my information privacy	☐	☐	☐	☐	☐
I usually trust people until they give me a reason not to trust them	☐	☐	☐	☐	☐
Trusting another person is not difficult for me	☐	☐	☐	☐	☐
To me, it is the most important thing to keep my information private	☐	☐	☐	☐	☐
My typical approach is to trust new acquaintances until they prove I should not trust them	☐	☐	☐	☐	☐
My tendency to trust other is high	☐	☐	☐	☐	☐

Q12. For each of the following statements, please rate the extent to which you agree with the statement (on a scale of 1-5, where 1 is strongly disagree and 5 is strongly agree):

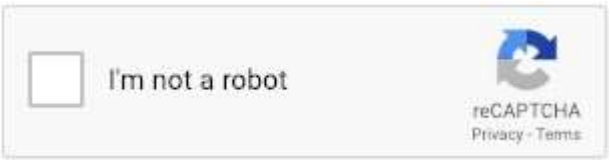
	1 Strongly disagree	2 Somewhat disagree	3 Neither agree nor disagree	4 Somewhat agree	5 Strongly agree
The government needs broader online surveillance authority	☐	☐	☐	☐	☐
The government needs to have more authority to use high tech surveillance tools for peoples online activities.	☐	☐	☐	☐	☐
The government needs to have greater access to individual bank accounts.	☐	☐	☐	☐	☐
The government needs to have greater access to personal information.	☐	☐	☐	☐	☐

Q13. Please rate your political outlook on a scale of 1-7, where 1 means very liberal, 7 means very conservative and 4 means moderate:

	1 Very Liberal	2 Liberal	3 Somewhat Liberal	44 Moderate	5 Somewhat Conservative	6 Conservative	7 Very Conservative
How would you describe your political outlook with regard to social issues such as marijuana legalization, abortion, personal freedoms and gay rights?	□	□	□	□	□	□	□
How would you describe your political outlook with regard to economic issues such as how governments should regulate trade and taxes, how much the government should tax income and whether the government should regulate businesses?	□	□	□	□	□	□	□

Q14. For each of the following statements, please rate the extent to which you agree with the statement (on a scale of 1-5, where 1 is strongly disagree and 5 is strongly agree):

	1 Strongly disagree	2 Somewhat disagree	3 Neither agree nor disagree	4 Somewhat agree	5 Strongly agree
I am aware of the privacy policies implemented by online sites that I use	□	□	□	□	□
I am aware that my personal information or communications could be made available to government agencies	□	□	□	□	□
I am aware of the wider issues around data privacy within the US from the news and other sources	□	□	□	□	□
I am aware of the types of information I have agreed that online sites can store about me	□	□	□	□	□



Here is your completion ID : ${e://Field/Random%20ID}_____

When you have copied this ID into Mechanical Turk, please click the next button to submit your survey.

Thank you for your participation in our study - we really appreciate your contribution. Please feel free to add any comments that may help us improve our survey. If you had any issues completing the survey please provide your worker-id and issue detail for investigation.

Appendix O. Matrix Totals for the CSR Reports

	Company	Control	Justice
1	3M	3	4
2	Aetna	2	0
3	AIG	1	4
4	Allstate	11	108.5
5	Alphabet(Google)	5	84
6	Amazon	2	15
7	American Airlines	2	4.5
8	American Express	19	53
9	Amerisource Bergen	1	0
10	Anthem	8	54.5
11	Apple	5	150
12	Archer Daniels Midland	0	0
13	AT&T	22	110
14	Bank of America	0	0
15	Berkshire Hathaway	0	0
16	Best Buy	28	56
17	Boeing	0	0
18	Cardinal Health	8	40.5
19	Caterpillar	0	0
20	Chevron	1	4
21	CHS	0	0
22	Cigna	16	74
23	Cisco Systems	3	128.5
24	Citigroup	11	55
25	Coca-Cola	0	0
26	Comcast	0	0
27	Conoco Phillips	1	18.5
28	Costco Wholesale	0	0
29	CVS Health	2	25.5
30	Deere	2	36
31	Dell	1	29.5
32	Delta Air Lines	9	24
33	Dow	0	0
34	Dupont	1	4
35	Energy Transfer	0	0
36	Enterprise Products	6	9.5
37	Express Scripts	0	0
38	Exxon Mobil	0	0
39	Facebook	0	0
40	Fannie Mae	0	0

41	FedEx	6	34
42	Ford Motor	18	68.5
43	Freddie Mac	0	0
44	General Dynamics	2	10
45	General Electric	4	13
46	General Motors	43	45.5
47	Goldman Sachs	5	9
48	Halliburton	0	0
49	HCA Healthcare	0	0
50	Home Depot	8	26.5
51	Honeywell	1	19
52	HP	10	180
53	Humana	11	0
54	IBM	1	100.5
55	Ingram Micro	5	27
56	Intel	6	49
57	Johnson & Johnson	1	4
58	JPMorgan Chase	0	0
59	Kroger	7	39
60	Liberty Mutual	9	35
61	Lockheed Martin	10	24
62	Lowe's	17	27
63	Macy /Sears	1	16
64	Marathon	3	0
65	Mass Mutual	0	0
66	McKesson	0	0
67	Merck	15	44
68	MetLife	6	13.5
69	Microsoft	1	108
70	Mondelez	0	0
71	Morgan Stanley	3	22.5
72	Nationwide	3	9.5
73	New York life	0	0
74	Oracle	5	13
75	PepsiCo	0	0
76	Pfizer	1	4
77	Phillips 66	0	0
78	Plains GP Holdings	0	0
79	Procter & Gamble	2	27.5
80	Prudential	3	25.5
81	State Farm	0	0
82	StoneX Group	0	0
83	Sysco	0	0
84	Target	5	23

85	Tech Data	1	4
86	TIAA	1	10
87	Tyson Foods	0	0
88	United Airlines	0	0
89	UPS	5	0
90	United Health	5	36
91	Valero Energy	4	0
92	Verizon	30	124
93	Walgreens Boots	0	0
94	Walmart	1	5
95	Walt Disney	4	14
96	Wells Fargo	6	36.5
97	World Fuel	1	19