Differences in Perceived Information Sensitivity During Smartphones Use Among UK University Graduates

Emmanuel Ocheme Ochoga

Faculty of Computing Engineering and Media

January 2021

A thesis submitted in fulfilment of the University's requirements for the Degree of Doctor of Philosophy

Declaration

To the best of my knowledge, I confirm that the work in this thesis is my original work undertaken for the degree of PhD in the Faculty of CEM, De Montfort University. I confirm that no material of this thesis has been submitted for any other degree or qualification at any other university.

Abstract

The level of sensitivity with which smartphone users perceive information influences their privacy decisions. Information sensitivity is complex to understand due to the multiple factors influencing it. Adding to this complexity is the intimate nature of smartphone usage that produces personal information about various aspects of users' lives. Users' perceive information differently and this plays an important role in determining responses to privacy risk. The different levels of perceived sensitivity in turn point out how users could be uniquely supported through information cues that will enhance their privacy. However, several studies have tried to explain information sensitivity and privacy decisions by focusing on single-factor analysis. The current research adopts a different approach by exploring the influences of the disclosure context (smartphone ecosystem), three critical factors (economic status, location tracking, apps permission requests) and privacy attributes (privacy guardian, pragmatist, and privacy unconcerned) for a more encompassing understanding of how smartphone user-categories in the UK perceive information. The analysis of multiple factors unearths deep complexities and provides nuanced understanding of how information sensitivity varies across categories of smartphone users. Understanding how user-categories perceive information enables tailored-privacy. Tailored privacy moves from "one-size-fits-all" to tailoring support to users and their context.

The present research applied the Struassian grounded theory to analyse the qualitative interview data collected from 47 UK university graduates who are smartphone users. The empirical research findings show that smartphone users can be characterised into eight categories. However, the category a user belongs depends on the influencing factor or the information (identity or financial) involved and the privacy concern category of the user.

This study proposes a middle-range theory for understanding smartphone users' perception of information sensitivity. Middle-range theories are testable propositions resulting from in-depth focus on a specific subject matter by looking at the attributes of individuals. The propositions shows that an effective privacy support model for smartphone users should consider the varying levels of

information sensitivity. Therefore, the study argues that users who perceive information as highly sensitive require privacy assurance to strengthen privacy, whereas users who perceive information as less sensitive require appropriate risk awareness to mitigate privacy risks. The proposition provides the insight that could support tailored privacy for smartphone users.

Keywords

Perceived information sensitivity; Smartphone users; Privacy; Tailored support.

Dedication

This thesis is dedicated to the Holy Spirit, My Helper who made it possible for me to start and to finish this research study.

Acknowledgement

I like to express my sincere gratitude to my supervisors, Dr Isabel Wagner, Dr Caroline Khene and Professor Bernd Stahl for their professional support and advice. I am equally grateful to Dr Ying He, who was my first supervisor and for her continued advice even after she left DMU.

My appreciation also goes to my examiners Dr. Jacques Ophoff (external examiner) and Dr. Laleh Kasraian (internal examiner) for their useful feedback. Additionally, I like to thank all of the participants interviewed in this study for their time and useful contributions. I would like to express my deep appreciation to my wife, Toluwase Victoria Olowu-Ochoga who supported me throughout, and to my children Agbenu and Emmanuella Ochoga for constantly asking: “daddy when are you finishing your PhD”. I like to also extend my gratitude to Nathaniel Odin for his invaluable understanding and support during this research work.

Table of Contents

CHAPTER ONE 14

1. RESEARCH INTRODUCTION AND CONTEXT 14

1.1 INTRODUCTION 14
1.2 MOTIVATION AND CONTRIBUTION 16
1.3 RESEARCH AIM 20
1.4 RESEARCH QUESTIONS 20
1.5 THE SCOPE OF STUDY 20
1.6 EPISTEMOLOGICAL AND ONTOLOGICAL POSITION 23
1.7 THESIS STRUCTURE 24

CHAPTER TWO 26

2. PRIVACY AND INFORMATION SENSITIVITY 26

2.1 INTRODUCTION 26
2.2 THE CONCEPT OF PRIVACY 27
2.3 DIMENSIONS OF PRIVACY 29
2.3.1 GDPR STANDARDS FOR PRIVACY PROTECTION 30
2.4 THE CONCEPT OF INFORMATION SENSITIVITY 33
2.4.1 FACTORS INFLUENCING THE PERCEPTION OF INFORMATION SENSITIVITY IN SMARTPHONE USE 35
2.5 THE CRITICAL FACTORS 43
2.5.1 SELECTION CRITERIA 43
2.6 CONCLUSION 46

CHAPTER THREE 48

3. DATA COLLECTION, PRIVACY RISKS AND USER CATEGORIES 48

3.1 INTRODUCTION 48
3.2 DATA COLLECTION IN THE SMARTPHONE CONTEXT 49
3.2.1 AUTOMATED AND SURREPTITIOUS COLLECTION 49
3.2.2 MOBILE CROWD SOURCING (MCS) 49
3.2.3 WEB SURVEY COLLECTION 50
3.3 PRIVACY IMPLICATIONS OF DATA COLLECTION 50
3.3.1 PRIVACY RISKS FOR AUTOMATED COLLECTION 50
3.3.2 PRIVACY RISKS FOR MOBILE CROWDSOURCING (MCS) 51
3.3.3 PRIVACY RISKS FOR WEB SURVEY DATA COLLECTION 52
3.4 USER RESPONSES TO PRIVACY RISKS 52

3.4.1 Information Seeking 53
3.4.2 Withholding of Information 54
3.4.3 Fabrication of Information 55
3.5 Smartphone Users' Categories 55
3.5.1 Users Characterisation by App Usage and Demography 56
3.5.2 Users Characterisation by Privacy Attributes 57
3.5.3 Alan Westin's privacy characterisation 58
3.6 Conclusion 60

CHAPTER FOUR 61

4. THEORETICAL FRAMEWORK 61

4.1 Introduction 61
4.2 What Is a Theory 62
4.3 Theoretical Framework as a Frame of Reference for Conducting Research Studies 63
4.4 Privacy Theories and Privacy Decisions 65
4.4.1 Rationality Theories and Privacy Decisions 65
4.4.2 The Control Theory of Privacy and Privacy Decisions 68
4.4.3 Restricted Access/Limited Control (RALC) and Privacy Decisions 70
4.4.4 The concept of bounded rationality and privacy decisions 72
4.5 Conclusion 75

CHAPTER FIVE 76

5. Research Methodology 76
5.1 Introduction 76
5.2 Philosophical Paradigms 76
5.2.1 Positivism 79
5.2.1.1 Criticism of the positivist paradigm 80
5.2.2 Interpretivism 81
5.2.2.1 Criticism of interpretivist research 83
5.2.3 Critical Research 84
5.3 The Rationale of Adopting Interpretivism for this Research 87
5.3.1 Research Approach 88
5.4 Research Methods 89
5.4.1 Ethnography 90
5.4.2 Case Study 91
5.4.3 Action Research 92
5.4.4 Grounded Theory 93
5.4.4.1 The Rationale of adopting grounded theory for this research 94
5.5 Data Collection Methods 95
5.5.1 Observation 96
5.5.2 Documents 97
5.5.3 Interview 97

5.5.3.1 The interview questions and respondents 99
5.5.3.2 Interview protocol 104
5.5.3.3 The Pilot study 105
5.5.3.4 Ethical Issues 106
5.6 THE ANALYSIS PROCESSES 107
5.6.1 DATA ANALYSIS: GROUNDED THEORY 107
5.6.1.1 Constant comparison 108
5.6.1.2 Theoretical sampling 108
5.6.1.3 Glaserian vs. Straussian strands of GT 110
5.6.1.4 Straussian GT procedures 113
5.7 THE VALIDATION PROCESS IN GROUNDED THEORY 115
5.8 COMPUTER-ASSISTED QUALITATIVE DATA ANALYSIS SOFTWARE (CAQDAS) 118
5.8 CONCLUSION 119

CHAPTER SIX 120

6. RESULTS AND FINDINGS 120

6.1 INTRODUCTION 120
6.1.1 PARTICIPANTS DESCRIPTION 120
6.1.2 THE CODING PROCESS 123
6.1.3 BUILDING OF THE THEORETICAL PROPOSITION 123
6.2 THE INFLUENCE OF ECONOMIC STATUS FROM THE HIGH-INCOME GROUP 124
6.2.1. THE IMPACT OF INCOMPLETE INFORMATION AND COGNITIVE LIMITATION 126
6.2.2 CREATION OF PRIVACY ZONE AMONG HIGH-INCOME GROUPS 129
6.2.3 INFLUENCE OF TIME CONSTRAINTS AMONG HIGH INCOME GROUP 132
6.3 THE INFLUENCE OF ECONOMIC STATUS FROM THE MIDDLE-INCOME GROUP 136
6.3.1 CREATION OF PRIVACY ZONE AMONG MIDDLE INCOME GROUP 137
6.4 THE INFLUENCE OF ECONOMIC STATUS FROM THE LOW-INCOME GROUP 142
6.4.1 THE IMPACT OF INCOMPLETE INFORMATION AND COGNITIVE LIMITATION 143
6.5 THE INFLUENCE OF LOCATION TRACKING FROM THE 3 PRIVACY CATEGORIES 149
6.5.1 THE INFLUENCE OF BOUNDED RATIONALITY REGARDING LOCATION TRACKING 150
6.5.2 CREATION OF PRIVACY ZONE REGARDING LOCATION TRACKING 152
6.6. THE INFLUENCE OF APPS PERMISSION REQUESTS FROM THE 3 PRIVACY CATEGORIES 156
6.6.1 THE INFLUENCE OF BOUNDED RATIONALITY REGARDING APP PERMISSION REQUEST 156
6.6.2 THE INFLUENCE OF RALC CONSTRUCTS OF CHOICE AND CONSENT 158
6.7 CONCLUSION 161

CHAPTER SEVEN 162

7. DISCUSSION OF VARYING PERCEPTIONS OF INFORMATION SENSITIVITY 162

7.1 INTRODUCTION 162
7.2 THE INFLUENCE OF ECONOMIC STATUS 162

7.2.1 CONCERN FOR IDENTITY 163
7.2.1.1. Concern for identity among privacy guardians (HI-PG, MI-PG and LI-PG) 163
7.2.1.2 Concern for identity among privacy pragmatist (HI-PP, MI-PP and LI-PP) 166
7.2.1.3 Concern for identity among privacy unconcerned (HI-PU, MI-PU and LI-PU) 168
7.2.2 CONCERN FOR SAFETY OF FINANCES 169
7.2.2.1. Concern for safety of finances among privacy guardians (HI-PG, MI-PG and LI-PG) 170
7.2.2.2 Concern for safety of finances among privacy pragmatist of all income groups (HI-PP, MI-PP and LI-PP) 171
7.2.2.3 Concern for safety of finances among privacy unconcerned from all income groups (HI-PU, MI-PU and LI-PU) 172
7.3 FURTHER DISCUSSION OF MAIN FINDING REGARDING ECONOMIC STATUS 173
7.4 THE INFLUENCE OF LOCATION TRACKING 177
7.4.1 FURTHER DISCUSSION OF THE FINDINGS REGARDING LOCATION TRACKING 181
7.5 THE INFLUENCE OF APP PERMISSION REQUEST 184
7.5.1 FURTHER DISCUSSION OF THE FINDINGS REGARDING APP PERMISSION REQUEST 187
7. 6 THE INFLUENCE OF BOUNDED RATIONALITY AND RALC THEORIES ON THE PERCEPTION OF INFORMATION SENSITIVITY 190
7.6.1 UNDERSTANDING USER SENSITIVITY PERCEPTIONS THROUGH BOUNDED RATIONALITY AND RALC 193
7.7 THE MIDDLE-RANGE THEORY FOR UNDERSTANDING SMARTPHONE USERS' PERCEPTION OF INFORMATION SENSITIVITY 194
7.8 CONCLUSION 197

CHAPTER EIGHT 198

8. RESEARCH CONCLUSION AND FUTURE RESEARCH 198

8.1 ANSWERS TO RESEARCH QUESTIONS 199
8.2 RESEARCH CONTRIBUTIONS AND IMPLICATIONS 202
8.2.1 THE PRACTICAL CONTRIBUTIONS AND THE IMPLICATIONS FOR PRACTITIONERS 204
8.3 LIMITATIONS OF RESEARCH 206
8.3.1 FUTURE RESEARCH 208
8.4 CLOSING REMARK 208

REFERENCES 210

APPENDIX A: ETHICAL APPROVAL 236

APPENDIX B: SAMPLE CONSENT FORM 237

APPENDIX C: WESTIN'S ORIGINAL INTERVIEW QUESTIONS AND THE ANALYSIS GUIDE.....238

List of Tables

Table 1.1: Recent Industry Reports of Data Breach Involving GDPR Enforcement Actions in the UK----------22
Table 4.1**:** Presents the Relevant Components of The Selected Theories----------74
Table 5.1: Comparison of IS Research Paradigms----------89
Table 5.2: Summary of The Research Methods Considered----------94
Table 5.3: The Semi-Structured Interview Questions for the First Round of Interviews----------100
Table 5.4: The Semi-Structured Interview Questions for The Second Round of Interviews----------101
Table 5.5: The Semi-Structured Interview Questions for The Third Round of Interviews----------102
Table 5.6: Summary of The Sources of Data----------103
Table 5.7: Characteristics of Interviewees and Labels----------103
Table 5.8: Revision of Interview Questions from the Pilot Study----------106
Table 5.9: Summarises the Main Differences Between Glaserian Vs. Straussian Approaches----------112
Table 6.1: Background Questions Prepared for Interview Participants----------122
Table 6.2: Summarises How High-income Categories Perceive Information Differently----------.125
Table 6.3**:** Emerged Concepts from The Open Coding Stage from the HI-Income Perspective.----------133
Table 6.4**:** Nodes/themes developed in open/axial/selective coding from HI-Income Respondents----------134
Table 6.5: Shows the Coding Process and Presents how Middle-income Categories Perceive Information ----------136
Table 6.6: Emerged Concepts from The Open Coding Stage from the MI-Income Perspective----------139
Table 6.7: Nodes/themes developed in open/axial/selective coding from MI-Income Respondents----------140
Table 6.8: Shows the Main Points from the Coding and How Low-Income Categories Perceive Information.----------142
Table 6.9: Emerged Concepts from the Open Coding Stage from the LI-Income Categories.----------147
Table 6.10: Nodes/themes developed from LI-Income Respondents----------148
Table 6.11: Emerged Concepts on Location Tracking from The Open Coding Stage Across Distinct Groups of Users----------153.
Table 6.12: Nodes/themes developed in open/axial/selective coding regarding Location Tracking----------154
Table 6.13: Emerged Concepts from The Open Coding Stage from Apps Permission Request----------159
Table 6.14: Nodes/themes developed in open/axial/selective coding process about Apps Permission Requests----------160

Table 7.1: A Summary of Findings Regarding Concern for Identity From 3 Perspectives.----------163

Table 7.2: A Summary of The Analysis Regarding the Concern for The Safety of Finances----------170.
Table 7.3: Summary of Main Findings and Contributions to Literature from Low-Economic Status Group.----------177
Table 7.4: Summary of Main Findings and Contributions Regarding Location Tracking----------183
Table 7.5: Summary of Findings and Contribution Regarding Apps Permission Request----------190
Table 7.6: Summarises the Guidelines Applied in Developing the Middle-Range Theory----------195

List of Figures

Figure 4.1: Illustrates the Relationships in The Theoretical Framework----------75
Figure 5.1: Paradigm Model in Axial Coding----------114
Figure 5.2: The Grounded Theory Process----------118
Figure 6.1. Framing of The Inquiry and Relationship Between Concepts---------123
Figure 6.2: Illustrates the Iterative Process of GT Leading to Data Saturation
----------124
Figure 6.3 Illustrates the Coding Process Regarding LT And APR----------150
Figure 7.1: Illustrates How Location Tracking Provide Different Insights Regarding Distinct Users----------178.
Figure 7.2: Illustrates the Core Category and Varying Influence of App Permission Request----------185
Figure 7.3: Integrated Theoretical Framework and Research Findings.----------191

Chapter One

1. Research Introduction and Context

1.1 Introduction

Information privacy is a major concern for smartphone users because of the potential loss of personal information (Cabalquinto and Hutchins, 2020; Mothersbaugh et al., 2012). Potential losses include identity theft (Jibril et al., 2020) and loss of financial information (Furini et al., 2019) which triggers information sensitivity. “Information sensitivity is the level of privacy concern an individual feels for a type of data in a specific situation” (Hong et al., 2019, p. 10).

Users perceive information differently and exploring the different perceptions provides insight for tailored privacy (Knijnenburg, 2017). Understanding how to tailor privacy support to different categories of smartphone users is important because more people access the internet through smartphones (Ketelaar and van Balen, 2018; Pennekamp et al., 2017). Tailored privacy adapts risk communication to match users’ level of sensitivity in order to improve their privacy (Knijnenburg, 2017). For example, information that highlights potential risks empowers users with low perception of information sensitivity to appropriately mitigate privacy risk (Gates et al., 2014; Mousavi et al., 2020). Privacy is a fundamental human right. However, in the big tech landscape, companies are increasing efforts that minimise users’ privacy. For example, Google was fined 50 million Euro under the General Data Protection Regulation (GDPR) for Android sign-up procedure that made it impossible for users to give informed consent to data collection (CNIL, 2019). Hence, users need effective privacy support (Kulyk et al., 2019).

Privacy decision making is complex (Barth and de Jong, 2017). Adding to its complexity is the intimate nature of smartphone usage which in turn influences how users perceive information (Ketelaar and van Balen, 2018; Kim and Koohikamali, 2015). Information sensitivity provides the basis for tailoring privacy support to users. This is because perceived information sensitivity level reveal how users will protect personal information. According to Mothersbaugh et al. (2012) users with greater information sensitivity enacted more stringent protection over personal information. Several factors such as location tracking (Cabalquinto and Hutchins, 2020) and app permission requests (Degirmenci, 2020) influence users’ perception of information sensitivity and privacy decisions in the smartphone context. Therefore, focusing on the critical factors surrounding smartphone use data collection and privacy decisions help to elucidate user responses. Data collection imposes privacy-decision making on users (Acquisti

and Grossklags, 2005). Usually, the decision to withhold or disclose personal information is influenced by several factors based on underlying information sensitivity (Beldad et al., 2011; Kokolakis, 2015; Mothersbaugh et al., 2012). The factors influencing the privacy decisions of the smartphone user include: (1) context, (2) information-type, (3) unauthorised collection of data, (4) convenience and benefits of using the device, (5) location tracking, (6) app permission requests, and (7) users' economic status. This decision process require support. However, factors differ in terms of how critical they are to individuals' privacy (Brough and Martin, 2020). Studies reveal that location tracking (Ketelaar and van Balen, 2018; Kokkoris and Kamleitner, 2020), apps permission request (Balebako and Cranor, 2014; Kulyk et al., 2019) and users' economic status (Rahmati et al., 2012; Sheehy-Skeffington and Rea, 2017) are among the critical factors influencing user's privacy decision in the smartphone context. The wide adoption of smartphones results in the massive production of personal data about many aspects of users' daily life (Berenguer et al., 2017).

Consequently, Perentis et al. (2017) argues that the ease with which these personal data could be collected represents privacy threat and influences users' perception of information sensitivity. Moreover, information sensitivity influences privacy decision making (Bansal et al., 2010b; Kokolakis, 2015). To deepen the understanding of this phenomenon, the concept of bounded rationality (Simon, 1982) and Tavani's (2008) RALC (the Restricted Access/Limited Control theory) are explored.

One critical implication of privacy decision is that any information made public cannot be made private again. Therefore, the importance of privacy has to do with the consequences of not having privacy (Westin, 1970). That is why Sipior et al. (2014) argues that future research must address the privacy concerns arising from smartphone use.

This chapter introduces the research study. It continues with the research motivation and contribution, that provides the various motivations of the study from literature. Subsequently, the questions that the research seeks to address are presented. Following this, the epistemology and ontology that underpins the study, including the methodology is summarised. Then chapter the discusses the summary of results revealed by each chapter. Finally, an outline of the thesis structure is presented.

1.2 Motivation and Contribution

One of the problems attributed to the rapid adoption of the smartphone is privacy (Berenguer et al., 2017; Guinchard, 2020). Data collectors increase privacy concerns surrounding the smartphone by taking advantage of improved smartphone technology such as opportunistic sensing (Kulyk et al., 2019; Park et al., 2019) to collect users' data. Concerns about privacy cause users to generalise suspicion to several apps and inhibit warranted disclosure that could be welfare-enhancing or that contribute to the overall digital economy (UK Government, 2017). For example, a nationwide survey conducted by Pew Research centre in the U.S shows that 54% of mobile application users decided not to install an app for requesting sensitive information, while 30% of users uninstalled apps for collecting personal information they do not wish to share (Boyles et al., 2012). Apps uninstallation due to privacy concern are prevalent in the mobile app space (Kulyk et al., 2019). Apps developers can be nudged to protect user's privacy and users can be supported in making privacy decisions (Acquisti et al., 2017; Kulyk et al., 2019). Therefore, nuanced user-centric propositions that is informed by how various user-categories perceive information sensitivity makes an important contribution to tailored privacy for smartphone users.

Studies (Zhao et al., 2016) found that the literature emphasised a simplifying assumption that all smartphone users are similar in privacy preferences. However, they found another strand of studies that identified different usage characteristics among smartphone users. These characteristics focused on apps usage such as the download and installation of apps (Li et al., 2015), daily interactions with apps (Bhih et al., 2016), average usage sessions in apps (Banovic et al., 2014) and in terms of how app usage differs with the context (Do et al., 2011). In addition, Jones et al. (2015), reveals the existence of three different kinds of smartphone user clusters (groups) in terms of app re-visitation patterns. Jones et al. (2015) differentiated the user-clusters based on their engagement time with the apps. They referred to them as (1) checkers, **(**2) waiters**,** and (3) responsives. Similarly, Banovic et al. (2014) identified three types of users based on duration and interaction type: glance (those who glance the lock screen most of the time), review (users consuming content and providing quick input) and engage (interactions often involving multiple applications). According to Church et al. (2015), these characterisations confirm the existence of different user sub-groups. Therefore, treating smartphone users as the same has led to a lack of reproducibility and generalisability in smartphone studies (Zhao et al., 2016). This implies that the preference of some categories of users may not be addressed by generalised privacy

protection support. Therefore, understanding the privacy sensitivities of different categories of users will inform a more relevant type of tailored privacy. Information sensitivity reveals underlying privacy preferences because it predicts privacy decisions (Kim and Koohikamali, 2015; Mothersbaugh et al., 2012). Information sensitivity in the context of this study refers to the potential loss associated with the disclosure of personal information due to perceived risk Bansal et al., 2016; Mothersbaugh et al., 2012).

Smartphones have sensors, apps and other types of connections that enables the collection of users' data (Can and Demirbas, 2015; Guinchard, 2020). Data collection in this context impose privacy decisions on users which exacerbates information sensitivity (Cabalquinto and Hutchins, 2020; De Cristofaro et al., 2011). However, little is known about how privacy-related attributes that indicates privacy dispositions, for example, the privacy fundamentalist and pragmatist (Knijnenburg et al., 2017) influence smartphone users' perception of information sensitivity (Bansal et al., 2010b; Cecere et al., 2015; Paine et al., 2007). The majority of studies in this area focuses on the impact of personal disposition such as the *Big 5* (Bansal et al., 2010b; Mothersbaugh et al., 2012) and other non-privacy attributes such as demographics (Li et al., 2015). A study of smartphone users across privacy-related attributes such as this research can provide this missing insight. The foundation for this type of study is found in Westin's (1987) studies. Westin categorised general online users (the world of desktop and large screen computers) into privacy fundamentalist, privacy pragmatist and privacy unconcerned. Privacy fundamentalists are concerned about the accuracy and uses of collected data. They support privacy rights as well as privacy-protecting frameworks. Similarly, privacy pragmatists are willing to share personal information with trusted parties in exchange for benefits, whereas privacy unconcerned individuals are less protective of personal information. This categorisation is useful for differentiating and studying the influence of critical factors on smartphone users. Therefore, Westin (1987) categorisation along with the restricted access/limited control theory (Tavani, 2008) and the concept of bounded rationality (Simon, 1982) will guide this study. The restricted access/limited control (RALC) theory assumes that individuals have limited control over personal information (Tavani, 2008). Using the limited control, individuals can restrict access to the information over which privacy zones of restrictions have been created. The concept of bounded rationality (Simon, 1982) refers to rationality constrained or "bounded" by cognition, incomplete information, and finite amount of time. In the privacy context, it

refers to how the bounds on rationality constrain a subject from fully understanding the consequences of sharing personal information.

Previous studies (Mekovec et al., 2017) used Westin's categorisation to study usage differences of online devices for private and business activities. Mekovec et al. (2017) conducted a quantitative survey and found significant differences in how the privacy fundamentalist and privacy unconcerned conducted many activities such as information searching online. Their study shows that Westin's categorisation is useful for interrogating user-categories regarding privacy related activities in varying context. Since context (Bansal et al., 2016; Mothersbaugh et al., 2012) impacts users' privacy decisions, the smartphone context that imposes another layer of differentiation on online users is an important context for applying the Westin's categories to examine the differences in perceived information sensitivity.

Previous studies present opportunities for investigating the different privacy concerns of smartphone users and how to support their privacy decisions. For example, Gu et al. (2017) and Kusyanti and Puspa, (2018) pointed out privacy concerns regarding app downloads. The underpinning insight is that privacy concern differs with individuals' attributes and context. However, it is unclear how critical factors influence varying levels of information sensitivity among smartphone user-categories. The literature suggests that smartphone users respond to different factors in different ways. For example, some users perceive location tracking as a form of digital surveillance and are highly concerned about sharing location information (Cabalquinto and Hutchins, 2020). This implies that studying users' perception of information sensitivity should be factor-specific across different categories of users.

The importance of investigating the influence of critical factors in this area have been pointed out. Martinez-Perez et al. (2015) found that location privacy is important. A violation of users' location privacy can reveal several other details, including who the users are, where they go, and who they spend time with (Almuhimedi et al., 2015). This is because the embedded GPS, Bluetooth, Wi-Fi, sensors and network connectivity of the smartphone allow users movements to be captured through location tracking (Guinchard, 2020; Ketelaar and van Balen, 2018). However, most studies on the effect of location tracking in the smartphone context follows the generalist view of users (Abbas et al., 2014; Almuhimedi et al., 2015). In other words, there are no differentiation of user-categories in the studies.

App permission request is another critical factor because app and the permission request mechanism allow large-scale data collection (Kusyanti and Puspa, 2018). Mobile apps are highly attractive due to their utility and convenience. However, apps are the main sources of data breach in smartphones (Abubaker et al., 2018; Gotz et al., 2017). The wide adoption of smartphones produces massive personal data regarding many aspects of life at a very intimate level. To protect user's information, smartphone operating systems (OS) rely substantially on the permission-based model to enforce restrictions on the operations that each app can perform (Boateng et al., 2019; Degirmenci, 2020). However, most users are unaware of the types of personal information collected by apps when permission is granted (Kulyk et al., 2019). That is why the GDPR (ICO, 2020), requires that data collectors enable users to give informed consent when apps ask for permission. This calls for effective privacy support that aligns with how users perceive information sensitivity. Like location tracking, app permission requests should be understood in terms of how different user-categories protect personal information from unwarranted access requests.

Users economic status is another critical factor influencing privacy decision making (Acquisti et al., 2015; Carrascal et al., 2013; Sheehy-Skeffington and Rea, 2017). However, the influence of economic status has not been given enough attention in the smartphone context. Rahmati et al.(2012) investigated this influence in the smartphone context and found that economic status is a strong determinant of smartphone adoption as well as how apps are installed and used. Therefore, it is important users economic status is explored to deepen the understanding of how users perceive information sensitivity (Schudy and Utikal, 2017). Furthermore, the literature suggests a connection between economic status and privacy decisions (Acquisti and Grossklags, 2005; Carrascal et al., 2013). Acquisti et al. (2016) reviewed several economic research studies on the value and regulation of information. They found that individuals protect or disclose personal information based on the economic value that they attach to personal information. The attached value depends on context (disclosure environment) and conditions (user attributes) which can either increase or decrease the value of privacy to the individual. Therefore, a study that sheds light on the effect of individuals' economic status on privacy decisions in the smartphone context makes an original contribution. Doing this sheds light on nuances surrounding privacy decisions.

Finally, Stuart et al. (2019) calls for group level analysis of privacy which locates common group characteristics. Doing this simplifies tailored privacy. Stuart et al. (2019) argues that information privacy is not adequately researched across different

group attributes and so recommends that future research should consider the group level analysis of information privacy. Therefore, a study that explores the varying influences of the critical factors of location tracking, apps permission requests, and economic status and that connects various group attributes such as the privacy fundamentalist, privacy pragmatist and the privacy unconcerned contributes new understanding. Moreover, these factors have not been combined in a single analysis before in the smartphone context.

1.3 Research Aim

The aim of this research is to understand the differences in perceived information sensitivity among smartphone users. Understanding how users perceive information provides insight for tailored privacy. To achieve this, the following research questions are addressed:

1.4 Research Questions

The study will answer the following research questions:

1. What are the critical factors that influence information sensitivity among smartphone users?
2. What categories characterise privacy concerns among smartphone users whose personal data is collected via mobile applications?
3. How do the identified critical factors influence the perception of information sensitivity among smartphone users based on their characterised privacy concern?

1.5 The Scope of study

This study focuses on the differences in perceived information sensitivity among UK smartphone users who are university graduates, with particular attention to understanding differentiated privacy support.

To enable the answering of the research questions, this researcher conducted a qualitative study through face-to-face semi-structured interviews to collect data from 47 UK smartphone users who have at least a university first-degree. Studies (Da Veiga and Ophoff, 2020) shows that UK citizens have very high level of privacy concern. The UK has a population of 66.4 million citizens in 2018 with the gender demography nearly balanced at 50.6% female and 49.4% male. However, only 42% of UK citizens have at least a university first-degree (Office for National Statistics, 2019). Gender and

education level are important factors affecting privacy concern as studies shows that women are more concerned about privacy than men (Baruh et al., 2017). Also, the level of education such as the possession of a university degree have been found to increase individuals' knowledge of privacy rights (Turow et al., 2008) which in turn influences the perception of privacy risk and information sensitivity (Bartsch and Dienlin, 2016). Therefore, university graduates are expected to perceive privacy risks with higher level of information sensitivity compared to non-university graduates. However, it is unclear how other factors may influence university graduates' perception of privacy. This explains why this study investigates other factors such as economic status, location tracking and app permission requests.

A large majority (78%) of the UK adult population (16+) use smartphones (Ofcom, 2018). This shows the important role the device plays in the digital economy and in the lives of citizens. However, a major concern with using the device is privacy (Cabalquinto and Hutchins, 2020). Privacy concerns results from discrepancy between online users' privacy expectation and the confidence users have about the privacy protection practices of data collectors (Da Veiga and Ophoff, 2020). However, the critical factors; economic status (Carrascal et al., 2013; Sheehy-Skeffington and Rea, 2017), location tracking (Almuhimedi et al., 2015; Technology, 2017), and app permission requests (Kulyk et al., 2019) identified through a structured literature review moderates privacy concerns. Essentially, the research focused on understanding the influences of the critical factors among three categories of users to identify the differences in perceived information sensitivity.

The evidence suggests that privacy concern by citizens in the UK is higher compared to other European countries such as France (RSA, 2019). More specifically, UK citizens are more concerned about identity theft resulting in financial loss (RSA, 2019). This suggests that results from privacy studies among UK citizens may not accurately apply in other countries. Despite having a comparatively higher privacy concern, studies shows that majority (63%) of UK citizens do not know their privacy rights under the relevant regulations (Ashford, 2018). However, more recent information from the UK Information Commissioner suggests that citizens are becoming more aware of their privacy rights judging from the reported 15% increase in data protection complaints in 2020 compared with 2019[1]. Although the UK has its Data Protection Act (DPA), the EU General Data Protection Regulation (GDPR) is discussed in subsection 2.3.1 because the DPA implements the GDPR in national law.

[1] ICO hails transformative year as average fine trebles (computerweekly.com)

Table 1.1: Recent industry reports of data breach involving GDPR enforcement actions in the UK

Recent Major Data Breaches in the UK				
Date	**Organisation**	**Records compromised**	**Description**	**Sanction**
Oct 2020	Experian	Millions of UK adults	Trading, enriching and enhancing personal data without subjects' knowledge	Enforcement notice to make changes
Nov 2020	Ticketmaster	1.5 million UK records	Failing to protect users' data from security breach by allowing chatbot on payment page	£ 1.25m
Oct 2020	British Airways	429,612	No adequate security protecting customers data	£ 20m Reduced from £183m
Oct 2020	Marriott	393m	Failing to keep customers data secure	£18.4 reduced from £99m

Sources: Computerweekly.com [2,3,4 and 5]

[2] ICO slams Experian over 'invisible' data processing (computerweekly.com)
[3] Ticketmaster fined £1.25m by ICO for failing to protect customer data (computerweekly.com)
[4] BA argues ICO data breach fine down to £20m (computerweekly.com)
[5] ICO slashes Marriott breach fine to £18.4m (computerweekly.com)

1.6 Epistemological and Ontological Position

This section gives an overview of the research epistemology and ontology that informs the choice of methods, procedures, and techniques that the researcher uses to conduct this study. The detailed description of the research methodology is presented in Chapter five.

The interpretivist epistemology is adopted for this study. This epistemology is appropriate where explanation of a phenomenon is sought from multiple perspectives of research participants. Since the interpretivist believes reality (ontology) is multiple and relative (Crotty, 1998), it fits the present research that aims to understand smartphone users' perception of information sensitivity from three privacy concern categories. These relative and multiple perspectives are impossible to understand independently of the social players (Dudovskiy, 2016; Walsham, 1995), therefore explanation grounded in participants' discourse is made possible by interpretivism.

The research method adopted is the Straussian Grounded theory (GT) approach. GT develop concepts from data to construct subjective meanings from research participants' views. This method fits the interpretivist epistemology as Corbin acknowledges that grounded theory aligns with the relativist ontology saying; "I realise there is no one 'reality' out there waiting to be discovered" (Strauss and Corbin, 1998, p. 10). This implies that social reality regarding how the different categories of smartphone users perceive information can be captured. Moreover, GT is suitable for "engaging a phenomenon from the perspective of those living it*"* (Corley, 2015, p. 1). The study's broad phenomenon which is privacy decisions is problematic and GT can look systematically into data to generate patterns of behaviour that are problematic for those involved (Tavakol et al. 2006). Therefore, GT is most suitable for this study.

Although other qualitative methods such the case study lend itself to a deep understanding of a phenomenon, the case study is not used in this research mainly because of the large number of respondents (47) involved in the present study. Creswell (2017) recommends that multiple case studies should not exceed four or five cases in total. The multiple number of respondents and the lack of a bounded system (case) to characterise the respondents (Yin, 2014) make the case study unsuitable for this study.

The semi-structed interview is used to gain in depth understanding of participants' perceptions regarding privacy concerns (Chirban, 1996; DiCicco-Bloom and Crabtree, 2006). The interview tool allows the subjective realities of the different participants to be captured by the researcher.

1.7 Thesis Structure

This study comprises eight chapters, chapter one introduces the thesis. It expressed the importance of understanding the different perceptions of information sensitivity which provides insight for tailored privacy. Furthermore, the chapter motivates the study and highlights the novel contributions that can emerge and finally presents an overview of the research methodology

Chapter two reviews the literature on information privacy, information sensitivity and smartphone use to gain insight into the conceptions of privacy and information sensitivity. It explores the privacy standards of the General Data Protection Regulation (GDPR) that is useful for understanding the conception of users' privacy. The chapter focuses on the literature that provides understanding of user interactions with the smartphone to determine the critical factors influencing users' perception of information sensitivity. It initially adopts a broad outlook on the factors, but then narrows down to the critical factors, by assessing seven different factors with a set of justified selection criteria.

Chapter three continues the literature review by exploring the literature on smartphone use data collection to gain insight into the various ways of collecting smartphone-use data. This also provides the understanding of the privacy risks that smartphone users face as a result of users' data collection. It examines the ways individuals respond to privacy risks posed by smartphone use data collection methods. Before investigating how different user-categories perceive information sensitivity, it is important to understand how users are currently characterised. Therefore, the chapter explores the various characterisation of individuals to understand how smartphone users can be characterised.

Chapter four explains the theoretical framework guiding the study. It explores four privacy theories to determine the theoretical framework needed as a guide and theoretical sensitivity for data collection and analysis. The chapter discussed four common theories applied by IS researchers and then selects two - the Restricted Access/Limited Control (RALC) and the Concept of Bounded Rationality.

Chapter five explains the research methods applied in this study. The research applied the Grounded Theory qualitative research method through a series of semi-structured interviews to extract the perceptions of participants. This helps to unearth hidden nuances surrounding the influences of the critical factors and privacy attributes. Another important aspect explored in chapter five is the issue of philosophical paradigms underpinning the research and the data collection as well as the analysis process. These were identified, critiqued and the selection of interpretivism was justified.

Chapter six presents the results and findings of the empirical investigations which were conducted through the iterative interview process of Grounded Theory. The interviews provided data for the factors that influences how participants perceive information sensitivity from three economic status groups and three privacy concern categories. It provides participants' profile in order to contextualise participants' responses. Furthermore, this chapter explains the coding process leading to the development of concepts and categories. The chapter also demonstrates how the theoretical framework structured the analysis.

Chapter seven provides the discussion of the different perceptions of information sensitivity from the empirical research data. It contextualises the emerged categories from chapter six as the basis for the discussion. Then it elaborates the findings in discussions structured around the critical factors investigated. It also explores how differences in perceived information sensitivity enables tailored privacy following the finding of how smartphone users can be characterised. Another important aspect of the chapter is the theoretical examination of the findings through the lens of the theoretical frameworks. Based on the analysis of the findings, the chapter presents the middle range theory for supporting tailored privacy among smartphone users.

Lastly, chapter eight outlines answers to the research questions and provides a summary of the research contributions and implications. Additionally, the limitations of the study and directions for future research were provided.

Chapter Two

2. Privacy and Information Sensitivity

2.1 Introduction

This chapter reviews studies that focused on privacy and information sensitivity and/or users' behaviour online including the smartphone context. The review aims to answer the first research question, which is:

- *What are the critical factors that influence information sensitivity among smartphone users?*

In order to achieve this aim, a structured survey of the literature was performed in Scopus because of its large collection. The review followed the guidelines of Jalali and Wohlin (2012). First, we defined the search plan (including backward snowballing), the inclusion and exclusion criteria; next, we selected three search strings for the literature search (perception AND information sensitivity OR user responses AND smartphones, privacy risk AND user responses AND smartphones, Information sensitivity AND mobile app OR mobile app use); finally, we analysed and synthesised the literature. The search range was 2010 to 2020 which found 145 papers that were reduced to 52 after excluding papers that focuses on technical solutions. The literature survey was used to develop an understanding of factors influencing the perception of information sensitivity online. This understanding informed the naming of seven factors influencing information sensitivity among smartphone users. Additionally, we use these insights to develop a set of criteria for selecting the critical factors influencing smartphone users' perception of information sensitivity. Therefore, the main issues discussed in this chapter are the concept and dimensions of privacy, the concept of information sensitivity and the various factors influencing it.

2.2 The Concept of Privacy

Privacy is one of the most enduring social issues associated with information technologies (Chuttur, 2009; Pavlou, 2011; Strickland and Hunt, 2005). The continuous evolution in information and communication technology has aroused interest in privacy research, bringing to light several conceptions of privacy. Warren and Brandeis's (1890) conceived privacy primarily as the right to be "left alone". According Beldad et al. (2011), this view of privacy is widely accepted. However, the present realities of ICT challenges the practicality of being left alone. For example, it is difficult for individuals who use pervasive communication technologies such as the smartphone to be "left alone" because the connectedness of the device increases the chances of collecting users' data which in turn makes it more likely to be reached by an actual person or "not to be left alone". This is the reason privacy is a big issue surrounding the use of the smartphone and thus necessitates the understanding of ways users could mitigate privacy risks.

Another conception of privacy is the notion of freedom from intrusion. In other words, privacy is conceived as being free from certain kinds of intrusions such as others possessing personal information about another person without consent (Panichas, 2014). This conception is similar to the concept of "being let alone". The absence of intrusion conforms with the expectations of privacy, because privacy is threatened or diminished as a result of intrusion into individuals' physical, psychological or informational space. The various types of intrusions result in a lack of consensus regarding the concept of privacy (Beldad et al., 2011). Moreover, the historical conceptions of privacy are challenged by new technologies. For example, privacy is the central concern regarding the use of the smartphone (Ketelaar and van Balen, 2018; Zhou et al., 2017). In other related areas, privacy concern is an important consideration for adoption and growth: social networks (Choi, 2016a; Li et al., 2016), e-commerce (Anic et al., 2019), m-commerce (Xiao et al., 2020), location sharing services (Kokkoris and Kamleitner, 2020; Technology, 2017). Therefore, online users face a dilemma: between enjoying the benefits accruing from sharing personal information or reducing the risk to their privacy (Beldad, 2015; Knijnenburg, 2017). This means that freedom from intrusion is difficult to attain where technologies make it possible for personal information such as location to be intrusively accessed in

ways that could compromise privacy. Hence, the conception of privacy as freedom from intrusion is fundamentally challenged by technologies. However, the concept of control over information dissemination and unauthorised access (Tavani and Moor, 2001) provides alternative conception of online privacy that addresses a wide range of privacy concerns that arise in connection with computers and information technology. Therefore, the restricted access and limited control conception of privacy (RALC) makes it possible for online privacy to be managed. Moreover, "privacy is not isolated freedom" (Simmel, 2007, p. 71). Hence, Fried (1984) criticises the notion of relating privacy to secrecy and argues that a person has privacy when he can limit the knowledge others possess about himself. Fried says that “privacy is not absence of information about us in the mind of others, rather it is the *control* we have over information about ourselves.” The right to control access to personal information is a fundamental human right (Council of Europe, 2010) that individuals must have. For example, Article 8 of The Human Rights Act,1998 guarantees the right to respect for private and family life, home and correspondences (EHRC, 1998).Therefore, the exercise of this right requires appropriate support.

According to Pavlou et al. (2011), advances in information technology have expanded opportunities for technical solutions to privacy concerns. These opportunities allow IS researchers to take a leading role in finding ways for practical application of technological solutions to mitigate privacy concerns. Bartsch and Dienlin (2016) and Zhou et al. (2017) argue that technology should give control over personal information back to individuals who own it. Furthermore, Schwartz and Solove (2011) argue that individuals and groups have the right to decide *when*, *how*, and *to what extent* information about them should be collected. The collection and unauthorised use of users’ personal information represents the main concerns of smartphone users (Ketelaar and van Balen, 2018; Yasaka et al., 2020). For example, users uninstall apps due to privacy concerns (Degirmenci, 2020) and if a large portion of a population does not participate in using a public health intervention app due to privacy concerns, such an intervention would have limited impact (Guinchard, 2020; Yasaka et al., 2020). Therefore, the understanding of a context-relevant conception of privacy will support the formulation of the appropriate support for

individuals. This explains why studies that seek to address how individuals could maintain control over personal information is at the core of information system discipline over the years (Pavlou, 2011). Thus far, this chapter has discussed different conceptions of privacy. Chapter four discusses these theoretical conceptions in more details. The following section looks at the different dimensions of privacy to show the dimension that this research applies.

2.3 Dimensions of Privacy

Clark (1997) and DeCew (1997) classified privacy into four dimensions. These dimensions are: (a) privacy of the person or physical privacy, which according to Clark is concerned with the integrity of the person's body. A violation of this dimension of privacy includes blood transfusion without consent and compulsory immunisation, (b) the privacy of personal behaviour such as sexual preferences and religious practices, (c) the privacy of personal communications. A violation of this dimension of privacy include surveillance or monitoring by others, (d) the privacy of personal data or information. This is often referred to as information privacy or "the right to selective disclosure" (Armando et al., 2015; Hirschprung et al., 2016). The privacy of personal communication and privacy of personal information in Clark and DeCew's classification can be merged into one. This is because ICT allows personal information to be communicated easily. Moreover, privacy breach arises when personal information is communicated to unintended parties. We refer to the combination of the privacy of personal communication and personal information as primary dimensions of information privacy (Capistrano and Chen, 2015; Schwartz and Solove, 2011). The secondary dimension includes inferences made from individuals' personal behaviour such as sexual preferences and religious practices. In a sense, all the 4 dimensions of privacy (Clark, 1997; DeCew 1997) are related to informational privacy because an inference from any of the dimensions, when communicated becomes a concern of informational privacy. Therefore, the restricted control over information privacy gives individuals the opportunity to prevent the automatic transmission of their data to other individuals or groups (Tavani, 2007).

The discussion of information privacy is particularly important in the context of the current research because of the magnitude of threat to information privacy from the

avalanche of technological possibilities that makes it easy for breaches such as, unauthorized data transfer, tracking, weakening of data security, and indirect or intrusive data collection to take place (Abbas et al., 2011; Fawaz and Shin, 2014; Strickland and Hunt, 2005). Since personal data have become an economic commodity (Wilson and Valacich, 2012), those who collect often sell them for marketing purposes without the consent of data subjects. There are also real concerns that collected personal data may not be adequately protected and unauthorised third parties might have access to them as many recent cases of data breaches have shown (Hern and Pegg, 2018).

The current research focuses on information privacy, which encompasses the ability to control the collection, use, and proliferation of information about oneself (Hui et al., 2006; Pavlou, 2011; Preibusch, 2013). Information privacy generally reflects the definition of privacy as informational self-determination (Westin, 1970). Beldad et al (2011) points out that other definitions of privacy relate to physical or spatial understanding of privacy, i.e., non-intrusion or seclusion aspects (Tavani, 2007). In reality, as socio-technical developments continue to evolve, the relationships between information, physicality, and expression are changing the meaning of privacy and the possibilities of privacy intrusions (Dinev, 2014; Vasalou et al., 2015). These situations make information privacy one of the most contested social issues of the information age (Armando et al., 2015; Schwartz and Solove, 2011). Despite the attack on information privacy by new technologies, information privacy remains a fundamental human right (Council of Europe, 2010). This right includes the right to control information about oneself. Therefore, it is comparable to the prima facie rights of self-determination (Nissenbaum, 2004). Hence, the GDPR provides protection for individuals' privacy by defining the standards for protection and control over personal information. These standards are examined next.

2.3.1 GDPR standards for privacy protection

The conception and protection of privacy are influenced by regulation (Solove, 2002; Wachter, 2018). Therefore, attention is paid to the GDPR (General data protection regulation), which is the data protection regulation in Europe since May 2018. This regulation imposes new standards for protecting users' privacy which in turn

influence how users perceive information privacy risk. GDPR in article 5 articulates seven key principles: lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality (security), and accountability (ICO, 2020). We shall discuss the relevant principles required for individuals to have meaningful control over personal data. Those principles emphasise the rights of individuals (smartphone users) to manage usage of their data. Specifically, the lawfulness, fairness and transparency, purpose limitation, and integrity and confidentiality (security) principles are discussed.

A. Lawfulness, fairness and transparency: The lawful bases for processing data are set out in Article 6 of the GDPR. There must at least be one lawful basis for processing personal data. For example, there must be subject's consent, or a contract, legal obligation to comply with the law, vital interest to protect someone's life, performing a task in the public interest, and for legitimate interests. Transparency in handling users' data has the advantage of building trust. Trust changes users' perceptions of intrusion which can impact on the conception of privacy. To build trust, GDPR seeks to help users retain control and oversight through ensuring that organisations show transparency in ways that users are aware of data collection and processing (Bansal et al., 2010b; ICO, 2020; Wachter, 2018).

B. Purpose limitation: Purpose limitation prescribes that personal data shall not be used in any way incompatible with the initial purpose of the collection. This purpose must be explicitly stated in privacy notices. Consequently, article 21 gives data subjects the right to object to data processing if the purpose of data processing is unacceptable. However, the weakness in purpose limitation is that users do not read privacy notices that states the purpose of collecting data (Milne and Culnan, 2004; Schaub et al., 2017). As Wachter (2018) argues, the GDPR seeks to improve this situation by stating that: "the information to be provided to data subjects may be provided in combination with standardised icons in order to give an easily, intelligible and clearly legible overview of the intended processing" (Wachter, 2018, p. 446). This

implies that short notices with icons are preferred over long privacy statements.

C. Integrity and confidentiality (security): The integrity and confidentiality principle – also known as the security principle ensures that appropriate security measures are in place to protect individuals' personal data. The combination of data integrity (trustworthiness of data) and confidentiality (protection from unauthorised access) results in data security. Data security is needed for protecting the content of eavesdropped data from being easily accessed. A fundamental tension exists between forces in data security: individuals' information privacy on the one hand, and cyber-attackers, economic interest of companies and state surveillance on the other. The realisation of this tension influences the conception of privacy in the technological age. As individuals lose more control over privacy in this age, a security failure would seriously compromise users' privacy. Fortunately, the rights-based approach of the GDPR aims to equip users with the necessary tools to manage information privacy (Acquisti et al., 2017; ICO, 2020; Wachter, 2018).

Data security offers the ground for privacy assurance whereas perceived weakness in data security heightens privacy concern (Mousavi et al., 2020). Privacy concern trigger perceived information sensitivity (Amit et al., 2020; Milne et al., 2017). Therefore, data should be collected in ways that align with the preferences of data subjects, otherwise disclosures could be inhibited. The GDPR provides meaningful standards for collection and protection of personal data by organisations. Personal data is valuable for organisations because it supports product development and customer service (Acquisti et al., 2013; Spiekermann et al., 2015). However, organisations should understand the differences in perceived information sensitivity of individuals in order to adopt strategies that can support privacy.

Previous studies (Morton and Sasse, 2014; Shih et al., 2015) reveal that requests for data that meet individuals' preferences reduce privacy concerns. Moreover, rewards mitigate privacy concerns (Hallam and Zanella, 2017; Lee et al., 2015). Therefore,

understanding individuals' preferences can support the offering of appropriate reward that mitigates information sensitivity.

The overall digital economy is enhanced when data is collected without intrusion (UK Government, 2017). Firms and users benefit significantly from the firm's ability to learn so much about their customers (Abakouy et al., 2019; Spiekermann et al., 2015). Datasets that differentiate market actors improve firms' understanding of customers and boost their ability to address specific target markets (Bhatnagar and Ghose, 2004; Morton and Sasse, 2014). Therefore, Spiekermann et al. (2015) suggests that firms should seek to understand customers without being intrusive. Furthermore, by understanding customers' behaviour in terms of differences in perceived sensitivity to data request, firms can improve data collection, or re-design privacy notices which can support user-oriented data collection (Acquisti et al., 2013; Alessandro Acquisti et al., 2015; Garrison et al., 2012). The next section will examine information sensitivity as a concept.

2.4 The Concept of Information Sensitivity

The concept of information sensitivity as an aspect of information privacy is growing in importance. Bansal et al (2010b) and Mothersbaugh et al (2012) argues that information sensitivity is one of the factors influencing individual's willingness to disclose personal information. This is because information sensitivity represents the level of risk perception, hence it increases along with privacy concern. As perceived sensitivity of information increases, users' willingness to disclose information or engage with apps decreases (Hong et al., 2019; Malheiros et al., 2013). Degirmenci (2020) found that when sensitive information is requested, it results in the following: (1) privacy concern significantly increases, (2) perceived control reduces, and (3) users refuse to install or uninstall apps. These suggests that information sensitivity triggers the negative effects of requesting for sensitive information. Sensitive personal information includes user's name, address, phone number, national insurance number and financial information (Hong et al., 2019; Martin-Consuegra et al., 2015). However, the GDPR defines special category data that reveals subjects' race, political opinions, genetics, religion, trade union membership and health status as sensitive data requiring special protection. Therefore, perceived information

sensitivity to the special category data is expected to be high as it reveals intimate aspects of people's lives.

The level of intimacy individuals associate with a particular type of information determines the value placed on the information (Milne et al., 2017). This in turn influences the potential loss envisaged and the level of information sensitivity attached (Bansal et al., 2010b; Mothersbaugh et al., 2012). In other words, the perception of information sensitivity derives from the intimacy attached to information perceived as riskier to disclose because of potential losses (Bansal et al., 2016; Lwin et al., 2007). Therefore, to accurately support disclosure, a user's level of information sensitivity should be ascertained (Knijnenburg, 2017). However, measuring information sensitivity is problematic because of the difficulty in assigning categorical measures to it. Therefore, the classification of information sensitivity as high and low by Capistrano and Chen (2015) addresses this difficulty. However, the classification does not account for the types of information that influences perceived information sensitivity.

Information sensitivity as an information disclosure antecedent is context dependent (Bansal et al., 2016; Lee et al., 2013;Mothersbaugh et al., 2012)). For example, users are less sensitive to the disclosure of personal information on social network platforms, than they are in the context of e-commerce transaction (Li et al., 2016; Lee et al., 2013). This implies that data subjects' perception is influenced by either the level of intimacy associated with the information or the disclosure context. Context-sensitivity of information explains why the smartphone context increases users' risk perception. For example, non-personal information like location information attracts high sensitivity in the smartphone context due to allowing intimate inferences about a smartphone user (Almuhimedi et al., 2015; Yasaka et al., 2020). The advanced functionality of smartphones makes the device attractive for data collection (Abdulazim et al., 2013; Can and Demirbas, 2015). Smartphone-use data collection threatens users' privacy through intrusions and malicious activities. Users' data can be captured by recording users' activities and tracking movements amongst others. The threats and vulnerabilities of the smartphone exacerbates the perception of information sensitivity (Choi, 2016a; Sipior et al., 2014). Sipior et al. (2014) named some risky behaviour of smartphone apps such as location tracking,

accessing contact list, identifying users or smartphone's unique identifier, recording in-app purchases, and sharing data with advertisers and analytics companies.

2.4.1 Factors Influencing the Perception of Information Sensitivity in Smartphone Use

The present digital revolution and the drive towards personalisation of marketing communication by businesses have increased the quest for individuals' personal information. Apart from the value of personal information as a resource for business competitiveness (Abakouy et al., 2019; Spiekermann et al., 2015), the ubiquity of the smartphone and malicious use of sensors have increased the ease with which data collectors can access peoples' personal information. Malicious use of sensors that overrides users' choice and consent nullifies the outcome of rational deliberation to withhold information. The characteristics of the technology, according to Choi (2016) creates the perception of vulnerability. These situations raise privacy concerns among smartphone users (Almuhimedi et al., 2015; Balebako et al., 2011; Junglas et al., 2008). The review of literature reveals 7 factors that influences information sensitivity among smartphone users. These factors are:

1). **Context**- Context here refers to the different situations and platforms that requires information disclosure by the smartphone user (Li et al., 2010), such as social media platforms (Beldad, 2015; Kim, 2016) and m-commerce or e-commerce (Anic et al., 2019; Martin-Consuegra et al., 2015). Generally, context influences information sensitivity. People communicate through information sharing, by discriminating what information to share, and with whom. In doing this, individuals vary information sensitivity with the sharing context. For example, information considered too sensitive to disclose in a gaming app might be shared with a friend in a dating app. This suggests that when context changes, information sensitivity also changes (Bansal et al., 2016; Mothersbaugh et al., 2012). The variability of sensitivity across different context shows that context impacts on the value users attach to information and defines the associated response to data requests (Acquisti, 2004a; Carrascal et al., 2013; Cvrcek et al., 2006; Kokolakis, 2015).

2) **Information type -** Individuals attach varying degree of intimacy to different types of personal information (Bansal et al., 2010b; Furini et al., 2019; Schwartz and

Solove, 2011). Information types in this context includes emails, payment card details, medical information, and others. Different types of information raise varying levels of sensitivity (Milne et al., 2017). For example, the wide deployment of mobile health apps such as fitness trackers, personal wellbeing and medical apps in the ecosystem represents privacy concerns to users in terms of managing sensitive information (Wagner et al., 2016). The information relating to health status are more sensitive in nature and how they are handled is a potential cause of privacy concern.

3) **Unauthorised collection of data** - Smartphone users risk the unauthorised collection of personal data (Kulyk et al., 2019; Milne et al., 2017). Data collectors use various approaches to collect these data, which affect users' responses by triggering privacy concerns. For example, data can be collected by opportunistically using smartphone and GPS sensors without user knowledge (Abbas et al., 2011; Wu et al., 2013). Unauthorised collection and use of data violate trust and results in data breaches. The concern about data breach influences information sensitivity more profoundly in smartphone use than with personal computers because of the numerous types of apps the smartphone user installs. The apps provide services that uses several types of personal information such as health and wellbeing information. Apps expose users to mobile malwares (Guinchard, 2020; Kulyk et al., 2019). Malware is a malicious programme designed to use a device without the owner's consent. Users are expected to make decisions that impact the security of the device and the privacy of personal information (Gates et al., 2014; Malheiros et al., 2013). This decision-burden increase information sensitivity among users (Spiegel and Silva, 2018).

4) Convenience and benefits of using the device - Smartphones provide users with many benefits that enhances users' daily lives (Sipior et al., 2014). For example, smartphones allow the sharing of information related to the social life of users. Given the ubiquitous connectivity of these devices, the privacy of users' social life may be threatened by data collection from social network sites (SNS) (Choi, 2016b; Rose, 2012). Maintaining privacy requires striking a balance between the many benefits of using the smartphone and protecting the intimate information that the smartphone can giveaway. Generally, the risk of privacy violations from data collection triggers a range of responses, including information seeking, information withholding, and

information fabrication (Beldad et al., 2011). Although a combination of unawareness, short-term need fulfilment, and the discounting of long-term negative consequences (Acquisti, 2004a) explains user responses, the smartphone's intimacy introduces another layer of complexity in terms of understanding user responses to information requests (Ketelaar and van Balen, 2018).

5) **Location tracking** – Location tracking refers to the collection of users' location information over time (Koohikamali et al., 2015). The problem with location tracking is that it is perceived as digital surveillance (Amit et al., 2020; Kokkoris and Kamleitner, 2020). Location tracking is a critical factor influencing the perception of information sensitivity among smartphone users (Almuhimedi et al., 2015; Sipior et al., 2014; Technology, 2017). This is because location tracking provides implicit information and allows other types of privacy to be invaded. Implicit information is information not provided by users directly but inferred from data (Wachter, 2018).

Several studies have determined why location tracking is critical in this context. According to Ketelaar and van Balen (2018) the smartphone enables location tracking because it is carried about. The increasing expansion of connectivity and advances in smartphone technology that combines many different functionalities into one device enables location tracking (Cecere et al., 2015; Ketelaar and van Balen, 2018). People are connected everywhere, meaning they can be followed everywhere also.

Location tracking is used positively and negatively. The rise in the use of social media applications that allow people to see where friends, family and nearby services are located (Beldad, 2015; Thomas et al., 2013) gives smartphone users social benefits as they share to be sociable (Beldad, 2015). On the other hand, location sharing services is risky because it accumulates the history of places visited (Aloudat et al., 2014; Thomas et al., 2013). This leads to concerns for profiling, unauthorised use and disclosure of real-time information. According to Kostakos et al. (2011), these could inhibit the acceptance of apps that depends on users' location information for functionality. The continuous tracking of users is referred to as "überveillance" (Michael and Michael, 2010, p. 10) which is prevalent because of the drive for users' real-time location data that provides information for real-time marketing and social

media platforms like Facebook, Twitter and Instagram. This situation exposes users to unsolicited surveillance and sharing of users' location information without their consent (Almuhimedi et al., 2015; Kim, 2016). Dobson and Fisher (2003) warned about the dangers of ‘geoslavery’, in which a person’s physical location is coercively or surreptitiously monitored.

Surreptitious acquisition of users’ location is carried out in several ways. First, through the mapping of Wi-Fi router location and harvesting Wi-Fi data (Wind et al., 2016). Smartphone users conserve mobile data or maintain connection to the internet through Wi-Fi connection when mobile data is exhausted. The harvesting of Wi-Fi data through location tracking is worrisome. More worrying is that users are presented with free public Wi-Fi and it is difficult to differentiate fraudulent ones from the genuine (Cheng et al., 2013; Wind et al., 2016). Furthermore, Cheng et al., (2013) warned of the danger associated with surreptitious tracking as a smartphone user can be identified through the unique MAC (media access control) address of his/her device. However, users who want to avoid being tracked can turn off the Wi-Fi of their devices. However, the precise location in modern smartphones can be obtained through GPS which is even more accurate and computed on the client (Korpilo et al., 2017). Alternatively, surreptitious tracking can be made a lot more difficult by solutions that can randomise the MAC address frequently which most new smartphones now allows. However, the challenge is that using such privacy enhancing features requires some level of privacy-related knowledge, that the average user may not have (Kokkoris and Kamleitner, 2020; Leith and Farrell, 2020). This makes the issue of providing support for users' privacy decision important (Kulyk et al., 2019).

Conversely, smartphone users sometimes consent to be tracked by friends and family or share their location with friends on social networking apps for social connection (Cheung, 2014; Fusco et al., 2012; Kostakos et al., 2011). However, Aloudat et al. (2014) and Lee et al. (2013) revealed that some social network apps misuse the shared location of users by selling them to advertisers for location specific advertising. This implies that users are not aware that their data are being accessed by third parties (Almuhimedi et al., 2015; Young and Quan-Haase, 2013). Location information when misused has serious consequences for the user. According to

Fawaz and Shin (2014) and Michael and Clarke (2013), the consequences include security-related or financial losses. Also, an employee could be sanctioned by a tracking employer. Finally, the concern for physical safety regarding location tracking influences information sensitivity (Kostakos et al., 2011). Therefore, Ghazinour et al. (2014) argue that finding ways to support individual's location privacy is critical.

6) **Mobile apps and apps permission requests**- Apps are computer programs that run on mobile devices such as smartphones and tablets (Kulyk et al., 2019). Olmstead and Atkinson, (2015) argues that apps and apps permission requests are at the centre of the smartphone privacy debate. This is because apps frequently request access to sensitive data, such as location and contacts (Wang et al., 2017). According to Wang et al. (2017) app permissions are the mechanism by which app developers disclose how an app will interact with users' device and personal information.

One challenge with the permission model is the considerable number of decisions that users are expected to make (Kulyk et al., 2019). For example, there were 235 distinct types of permissions sought across 41 different categories of apps on the Google Play Store, ranging from social networking and finance/business to gaming. Averagely, each app in the Play Store requires five permissions before a user installs it, aside other run-time permission requests (Huebner et al., 2020). This is decision-burden on users and they exacerbates the feelings of uncertainty. Therefore, users should be supported to make more informed decisions regarding their privacy when choosing to install or use smartphone apps (Kulyk et al., 2019; Spiegel and Silva, 2018). If users make wrong privacy decisions, it can compromise strong security measures in the mobile systems. However, some operating systems such as Android rely on users to understand the permissions that an app is requesting and to base the installation and usage decision on the list of permissions that is presented (Kulyk et al., 2019; Liu et al., 2016). This situation is problematic to users since they are unable to estimate the risk of disclosure (Kulyk et al., 2019). Sipior et al. (2014) and Wang et al. (2017) argue that app permission request is one of the critical factors influencing privacy decision in this environment. For example, about 30% of app users reversed earlier permission and uninstalled an app, because it accessed personal data beyond the permission granted (Kusyanti and Puspa, 2018). This

explains why users are more cautious with installing apps when better informed. For example, when risk-score information is included in app permission, users avoided apps with high-risk scores (Acquisti et al., 2017; Gates et al., 2014; Kulyk et al., 2019)

Improving privacy decisions by users involves taking into account factors that influence a user's sensitivity perception and decision making (Kim and Koohikamali, 2015; Markos et al., 2017). Also relevant is how risk is communicated. Communicating risk to users accurately improves the choices that users make (Hatamian et al., 2019; Gates et al., 2014; Van Wassenhove et al., 2012). Studies reveal that permission descriptions are confusing or difficult to understand by many users (Felt et al., 2012) as nearly all apps requesting permissions come with some associated risk (Gates et al., 2014). In addition, Gates et al. (2014) developed risk scores that indicate which apps presents lower-risk or high risks to users. Gates et al. (2014) argue that if users prefer lower-risk apps, it will incentivize developers and data collectors to follow the least-privilege principle and request only necessary permissions. Most high-risk apps contain invasive advertisements (Martin-Consuegra et al., 2015) and they ask for permissions that are not relevant to functionality (Kulyk et al., 2019).

6a) **Malicious practices in mobile app ecosystem -** Recent research suggests an increase in malicious practices within the apps space which further complicates users' ability to give appropriate permissions. Choi et al. (2015) and Rastogi et al. (2016) report a malicious trend in the app market referred to as apps repackaging. Through app repackaging, hackers repackage popular apps by adding or replacing advert networks and malicious codes to the app before releasing it to the market. Through this disguise, hackers collect the personal information of users.

However, app markets have taken some countermeasures to address these malicious trends. These countermeasures include sandboxing and runtime permissions. Sandboxing isolates apps from accessing critical resources in the device. This is an additional layer of security to prevent apps from stealing data. Unfortunately, sandboxing can be bypassed by apps colluding to execute composite permissions which allows them to leak data. Although the Android OS checks if an app is accessing a permission-protected resource through another app, some

malicious apps can go undetected (Boateng et al., 2019). Similarly, runtime permissions have not been successful in providing privacy assurance to users (Huebner et al., 2020). The challenge with the runtime permission is that it is too coarse-grained (ignoring specific details), and the user might not be aware of the full implications when granting the permission (Degirmenci, 2020). Moreover, after granting permission, there is no way to restrict a malicious app from stealing data. The actual problem lies in the inability of users to correctly judge the acceptance of permission, thus raising uncertainty. Uncertainty results in permission sensitivity among some users (Degirmenci, 2020; Knijnenburg et al., 2017; Zhou et al., 2017). This shows the need to provide tailored support to distinct users because of too many permissions (Knijnenburg, 2017). Most repackaged apps ask for more permissions compared with the original version. Therefore, it is possible to detect apps repackaging by understanding various permissions (Rastogi et al., 2016). This is possible when a discerning user can identify two or more apps that are similar. That is why Rashidi et al. (2016) suggests that only expert users can make such savvy comparison to detect a repackaged app and prevent personal information leakage. This emphasises the critical influence of app permission request on smartphone users. Generally, apps permission requests are intended to give users the ability to restrict or allow how and what personal information is accessed (Degirmenci, 2020; Olmstead and Atkinson, 2015). Therefore, studies should seek to understand how permission request interacts with other factors such as diverse privacy attributes to affect a user's choice (Benton et al., 2013; Bhih et al., 2016).

7) **Users' economic status** – Users' economic status in our context refers to the net-income of smartphone users (Office for National Statistics, 2017). Smartphones have ubiquitous sensors that captures diverse personal information which can be linked to reveal users' economic status. For example, the smartphone captures users' purchases (Van Heerde et al., 2019). History of purchases reveals users' income segment (Zorbas et al., 2020). Users could suffer economic, social and other forms of discrimination through economic status profiling (Wachter, 2018). These possibilities raise privacy concerns that in turn influences the perception of information sensitivity. Therefore, economic status is an important factor influencing peoples' perception and use of technology (Goel et al., 2012; Kim and Koohikamali,

2015). This includes the perception of information sensitivity among smartphone users (Kim and Koohikamali, 2015; Rahmati et al., 2012). Similarly, Goel et al. (2012) found that economic status influenced how frequently web pages were accessed. Users of lower economic status accessed the web more than higher economic status users. Furthermore, Rahmati et al. (2012) argue that lower economic status individuals without access to other technologies used their iPod Touch more for activities commonly executed on PCs. Therefore, studies have shown the link between economic status and engagement with IT. In the smartphone context, low economic status users are conscious of monetary losses and thus more careful with monetary transactions compared to high economic status users (Magsamen-Conrad, 2014; Rahmati et al., 2012). This shows economic status as a distinguishing factor in information related behaviour. Therefore, a study of individuals' privacy behaviour that neglects users' economic status is missing valuable insights (Sheehy-Skeffington and Rea, 2017; Wachter, 2018).

There is a relationship between economic status and privacy decision making (Acquisti and Grossklags, 2005; Carrascal et al., 2013; Sheehy-Skeffington and Rea, 2017). For example, low economic status individuals focus on satisfying immediate needs. Therefore, they are likely to make satisficing privacy choices to alleviate their present situation (Sheehy-Skeffington and Rea, 2017; Simon, 1982). Understanding the relationship between economic status and different smartphone user-categories in terms of how their perception of information sensitivity varies has implications for businesses, policy makers and researchers (Acquisti et al., 2013; Alessandro Acquisti et al., 2015). According to Acquisti et al. (2015) when businesses understand how individuals in various economic classes protect personal data, managers can turn well segmented privacy-enhancing initiatives into a source of competitive advantage. From this, managers can understand the triggers of privacy risk in order to avoid it. In addition, it is important to policy makers because it will assist the development of segmented support for individuals of different economic classes. Furthermore, it will be possible for researchers to formulate more nuanced and granular views of privacy protection and data sharing associated with economic classes (Acquisti et al., 2013). In other words, understanding the nuances across economic status contributes to better privacy support for users. A study that highlight

important differences across users can influence interface designs (Jeong et al., 2016). Moreover, exploring the relationship between economic status and information disclosure in this context provides insight about privacy expectations of smartphone users in the overall digital economy (Bélanger and Crossler, 2011; Bhih et al., 2016; Gao et al., 2019). Understanding the influences of economic status is very important to the digital economy (Abakouy et al., 2019; UK Government, 2017). It shows varying sensitivity perceptions by pointing out the distinctive preferences of users (Kim and Koohikamali, 2015; Sheehy-Skeffington and Rea, 2017).

2.5 The Critical Factors

Some factors are critical in this context because they either determine or compromise other factors or have not been given sufficient attention. The structured literature review shows that location tracking, app permission request and economic status are the critical factors influencing users' perception of information sensitivity in the smartphone context. These factors strongly influence why and how users perceive privacy risks. However, in selecting the critical factors, other factors are assessed by applying the selection criteria.

2.5.1 Selection Criteria

To make the analysis of empirical data easier to understand, while still providing a similar level of insight, only the critical factors are selected for investigation in the empirical study. Each of the critical factors should fit at least two selection criteria. The five selection criteria are carefully articulated and selected based on the understanding accumulated from the structured literature review (see section 2.1). The credibility of the resultant theoretical propositions is dependent on the credibility of the factors from which it is derived (Inayat et al., 2015), therefore, the selection criteria are justified below.

1. The factor can yield implicit information about the user. As mentioned earlier, Implicit information is inferred information (Wachter, 2018). Implicit information includes user persona segment, workplace, or nearby shopping centre. A factor that leads to inferences about a user offer grounds for profiling which can result in discrimination.

2. The factor reflects and imposes the core characteristics of the smartphone. Liu and Yu (2017) identified the smartphone characteristics (running of applications) and connectivity (connection to internet) as the critical factors influencing the use of the smartphone. These factors influence the perceived usability and in turn allows the core characteristics of the smartphone to directly impact users' privacy (Zhang et al., 2010).
3. The factor allows users to restrict access and have limited control over privacy. A factor that moderates the effects of perceived information privacy risk is critical in any context (Yin et al., 2015). The restricted access and limited control theory (RALC) indicate that users manage privacy by restricting access and limiting control over information (Tavani, 2008; Tavani and Moor, 2001). Therefore, the mechanism that enforces restrictions around smartphone users' information privacy is critical (Armando et al., 2015; H. Wang et al., 2017).
4. The factor is a major concern among smartphone users (Almuhimedi et al., 2015; Amit et al., 2020; Boateng et al., 2019; Degirmenci, 2020).
5. The factor influences decision making but its influence on privacy decision making is insufficiently investigated in the smartphone context. Schudy and Utikal (2017) argue that more factors should be explored to provide new insight about individuals' privacy decision making.

Context: Context can yield implicit data, because contextual usage can be tracked, and inferences made (Wachter, 2018; Yang et al., 2017). Contexts consist of attributes such as physical location, computing environment, state of mind, cultural setting, and many other features. However, location tracking is separated from context because the challenges associated with context are with its distinct components. Moreover, context here refers to various platforms and applications (Mousavi et al., 2020; Yang et al., 2017). Context as a factor satisfies the first criterion. However, context tracking is not a critical issue in smartphone usage like location tracking (Kokkoris and Kamleitner, 2020; Yang et al., 2016) and permission request (Boateng et al., 2019; Degirmenci, 2020).

Information type: Users' sensitivity vary with information-type which in turn moderates information disclosure (Milne et al., 2017). This moderating effect allows users to restrict access and have limited control over personal information. Therefore, the factor of information-type satisfies the third selection criteria. However, it does not satisfy any other criteria (first, second, fourth and fifth).

Unauthorised collection of data: Unauthorised collection of data is a major concern for smartphone users and features prominently in literature (Amit et al., 2020; Kulyk et al., 2019). Most unauthorised data collection is for the explicit information it yields about a user (Gustarini et al., 2016). However, data collected this way can be applied maliciously in ways difficult to determine (Wachter, 2018). A mechanism for minimising this type of collection is apps permission request (Cabalquinto and Hutchins, 2020; Liu et al., 2016). Therefore, app permission request is selected as a critical factor because it helps to manage unauthorised collection of smartphones use data. Hence, unauthorised collection of data satisfies only the fourth selection criterion.

Convenience and benefits of using the device: The convenience of using the smartphone make users perceive information as less sensitive (Lee et al., 2013; Patriana Ch et al., 2015). It imposes the benefitting aspect of the device and moderate privacy risk. In this sense, convenience and benefits fits the second selection criteria, which relates to imposing the core characteristics of the smartphone on users. However, the factor is not critical because it does not match any other criteria very well.

Location Tracking: Location tracking is a major concern among smartphone users as already discussed. It also yields implicit information as location tracking can giveaway other types of information about the user (Amit et al., 2020; Technology, 2017). Additionally, it reflects and imposes the core characteristic of the device on users. Therefore, location tracking fits three (first, second and fourth) selection criteria. Hence, it is one of the three critical factors.

App Permission Request: The phrasing of app permission influences privacy decisions (Knijnenburg et al., 2017). Accepting wrong permission results in unauthorised access and secondary use of data (Boateng et al., 2019; Degirmenci, 2020; H. Wang et al., 2017). Additionally, permission requests are a gateway to users' information and thus reflects the core characteristic of the smartphone. Through the mechanism of app permission, users have potential control over privacy. Additionally, app permission regulates contextual disclosure and context moderate information-type sensitivity (Bansal et al., 2016; Mothersbaugh et al., 2012). Based on the aspects mentioned here, app permission satisfies the second and third selection criteria. Therefore, it is one of the three critical factors.

Users' economic status: Economic status is a major influencer of individual decision making which can help the understanding of users' privacy decisions (Carrascal et al., 2013; Sheehy-Skeffington and Rea, 2017). Additionally, it offers ground for profiling, discrimination, and inferential analytics (Gao et al., 2019). Moreover, it has not been sufficiently researched in smartphone users' privacy decision making as our structured literature reveals. Therefore, users' economic status satisfies the first and fifth selection criteria. Hence, it is one of the critical factors.

2.6 Conclusion

This chapter begins the review of literature for the research. It focuses on reviewing the various conceptions of privacy and information sensitivity. In addition, it discusses the factors influencing the perception of information sensitivity of smartphone users. This review enabled the identification of the critical factors in this area. The main objective of this review was to answer the first research question of this study, that is, *what are the critical factors that influence information sensitivity among smartphone users?*

The question sought to investigate and identify how the smartphone technology and the ways users interact with it may condition information sensitivity through the influential factors. Through this review, the different factors influencing information sensitivity among smartphone users including the critical ones have been identified.

These are context, information-type, unauthorised access, and the convenience and benefits of using the device. However, the critical ones are location tracking, app permission request and users' economic status.

Finally, the selection criteria were pointed out to clarify the critical factors. The influences of the critical factors will be investigated in the empirical study to determine how smartphone users could be characterised based on differences in perceived information sensitivity. The next chapter (chapter 3) continues the literature review and focuses on the current characterisation of smartphone users.

Chapter Three

3. Data Collection, Privacy Risks and User Categories

3.1 Introduction

This research aims to understand the differences in perceived information sensitivity among smartphone users. Perception of information sensitivity is how users perceive and respond to information privacy risks. Accordingly, this chapter draws from information privacy literature to gain insight into the ways of collecting smartphone use data with the view to understand the variety of privacy risks that smartphone users face. Additionally, it examines the ways users respond to the risks posed by data collection methods and explores the privacy characterisation of individuals to determine how smartphone users can be characterised. Privacy decisions are strongly influenced by the perception of sensitivity to information and privacy requests (Knijnenburg et al., 2017). Information sensitivity determines how users mitigate privacy risk, which is connected to the privacy attributes of different user-categories.

Although there is abundant literature on individuals' responses to privacy risks, the perspectives on privacy responses are generalised (Beldad et al., 2011). Thus, nuanced understanding of how to support varying users in the smartphone context is lacking (Knijnenburg et al., 2017). The present chapter overviews literature to understand the connections between data collection methods, privacy risks and user responses. This provides insights for empirical data analysis that points out how user-categories differs in perceiving information sensitivity.

The chapter has six main sections, section 3.1 provides the introduction. Section 3.2 presents the various methods for collecting smartphone use data. Section 3.3 discusses the privacy implication of the data collection. Section 3.4 focuses on user responses. Section 3.5 discusses user categorisations, and the final section 3.6 provides the conclusion of the chapter.

3.2 Data Collection in the Smartphone Context

Smartphone users risk the unauthorised collection of personal data. Data collectors have various options for collecting data, which triggers privacy concerns (Bouwman et al., 2013; Cabalquinto and Hutchins, 2020). Smartphones allow the capturing and storing of users' personal information that could be collected by third parties. Several sensors allow the collection of previously difficult-to-collect information, thus threatening privacy in ways not previously considered (Cabalquinto and Hutchins, 2020; Wachter, 2018). Therefore, users risk the privacy of personal information (Bouwman et al., 2013; Kulyk et al., 2019). The right to control and decide what personal information is shared is minimised. To enable accurate understanding of how users, perceive and respond to privacy risk, it is necessary to first identify the data collection methods that potentially trigger privacy risks.

3.2.1 Automated and Surreptitious Collection

Automated user data collection refers to the continuous collection of data through interactions with the embedded sensors once the app has been installed. Since collection is automated, user consent is not required each time data are collected (Köping et al., 2018; Korpilo et al., 2017). This situation challenges informational privacy by making it difficult to protect personal data, because automated collection may result in the unwarranted and surreptitious collection of personal data. This situation results in users feeling vulnerable to privacy breach (Boateng et al., 2019). Most automated and surreptitious smartphone use data collection are through apps that users installed in the device. This type of data collection is the most popular option, as it allows for large-scale data collection. Mobile apps are highly attractive because of their utility and convenience.

3.2.2 Mobile Crowd Sourcing (MCS)

MCS is the use of mobile devices such as smartphones by data collectors in the participatory sourcing of information. This approach exploits crowd wisdom and uses individuals as *sensors.* In participatory sensing, users are directly involved in sensing and reporting the action, for example, traffic situation in certain locations. Smartphone users are able to choose what data to share with the crowdsourcing

system and when to share it (Cai et al., 2018; Y. Wang et al., 2016). However, there is risk about dishonest use of shared information by the holding party (Cai et al., 2018). Unlike automated data collection, which is opportunistic and uses smartphone sensors to capture data without informed consent, MCS depends on the user's choice and consent to share information. There is significant concern about privacy when automated collection is used, however the mechanism of choice and consent (Acquisti et al., 2017) allows users to moderate this concern in the MCS scenario. In automatic sensing, the user is not aware of active apps (Wang et al., 2016).

3.2.3 Web Survey Collection

Web survey collection is another approach for data collection wherein data are gathered in the absence of face-to-face contact (Couper et al., 2018; Rendina and Mustanski, 2018). Smartphones have been used in various studies and interventions, as they allow researchers to readily connect with respondents. For example, this option has been used to collect data from the users of a mobile anesthesia calculator app (O'Reilly-Shah, 2017). Many survey platforms such as the site SurveyMonkey are optimized for mobile devices, thus allowing data collectors to reach many users. However, the effectiveness of web survey collection is influenced by how intensively the data subject uses the device. Studies indicate that those who use their devices more intensively are less likely to participate because of concerns regarding privacy (Wenz et al., 2019).

3.3 Privacy Implications of Data Collection

As mentioned in 3.1 and 3.2, data collection influences how users perceive information sensitivity in mobile applications. This in turn, conditions the privacy risk perceptions of the subjects. The privacy risks related to smartphones have been identified. Eckhoff and Wagner (2018) categorised five types of privacy risks which are: privacy of location, privacy of behaviour and action, privacy of media, privacy of the state of the body and mind, and privacy of social life.

3.3.1 Privacy Risks for Automated Collection

Automated data collection methods such as the opportunistic sensing for capturing human mobility data to obtain insights on urban transportation systems (Alexander

et al., 2015) triggers a range of privacy concerns among users. For instance, user location privacy is at risk if mobility data are being captured (Wang et al., 2010, 2012). The misuse of this location information may expose the user to physical harm. It also raises concerns regarding the privacy of the state of body and mind, as demonstrated by the monitoring, capturing, and reporting of the healthcare and psychological conditions of smartphone users via apps (Cornet and Holden, 2018). The misuse of this information may result in social segregation. Another concern is the concern for the privacy of social life, which is related to the social interactions of users (Eckhoff and Wagner, 2018), since SNS (social network sites) such as Facebook and Instagram are mostly used on smartphones (Conti et al., 2012). A violation of this privacy may lead to valuable information being shared, which could be used for targeted advertisements, such as political advertisements based on the user's political views.

Most automated smartphone use data collection are executed through mobile apps. Apps pose privacy risks regarding the leakage, manipulation, and loss of information (Grundy et al., 2017; Zhang et al., 2018). Although permission requests from apps allow users to regulate access to data and device resources (e.g., control over the camera) and confidential information (e.g., access to the contacts list), apps still present privacy risks. Studies suggest that most users are unaware of the data collected by apps (Almuhimedi et al., 2015; Wang et al., 2016). Nevertheless, users sometimes behave paradoxically by granting apps unwarranted permissions because they are unaware of information collected by apps (Degirmenci, 2020). Another possible explanation for this paradox is that smartphone users are unaware that different types of information may be aggregated within an app family (Facebook owns Instagram and shares data) to form a more precise profile of users.

Generally, because users are unaware of the extent of the data collected by apps (Harari et al., 2016; Kulyk et al., 2019), apps potentially pose several privacy risks. Privacy risks come with privacy concerns. These concerns, in turn, affect information disclosure (Malheiros et al., 2013; Mothersbaugh et al., 2012).

3.3.2 Privacy Risks for Mobile Crowdsourcing (MCS)

MCS is a cost-effective and scalable way of gathering difficult-to-access data

(Martinez-Balleste et al., 2013; Pournajaf et al., 2015). Because participation in MCS is voluntary, users choose when and what to share. Therefore, the privacy concern is minimal. However, the reported information could identify the reporter (e.g., reports of traffic conditions could contain location and movement information). Such scenarios present a privacy risk. However, anonymity and confidentiality could be ways of addressing this risk. While anonymity preserves the individual's identity, confidentiality preserves the disclosed content in the crowdsourcing system. Without the effective use of anonymity and confidentiality, a breach of privacy could threaten users' social life and their privacy of behaviour and action. For example, the information reported may be used to identify the reporter and threaten their social relationships (Cato et al., 2016; Huckvale et al., 2015).

3.3.3 Privacy Risks for Web Survey Data Collection

Sensitive data may be collected through mobile web surveys. Therefore, users' willingness to participate in surveys is influenced by their trust in the app's creator (Rendina and Mustanski, 2018). For example, the user's sexual orientation could be requested. Therefore, privacy risks posed by this type of collection exposes smartphone users who participate to possible embarrassment and discrimination. Although anonymity and confidentiality could address this concern, the potential for reidentification can threaten the privacy of behaviour and action (Cato et al., 2016).

3.4 User Responses to Privacy Risks

Generally, data collection triggers privacy risks and imposes privacy-decision making on users. Users perceive risks based on their level of control during data collection (Balebako and Cranor, 2014; Kulyk et al., 2019). Usually, the decision to withhold or disclose personal information is informed by the evaluation of risks/benefits of disclosure based on underlying preferences (Acquisti et al., 2015; Acquisti and Grossklags, 2005). Users are offered free services or information by data collectors in exchange for valuable information. Some of these "free" services include content from third-party developers. Users therefore face the risk of inappropriate access and the use of personal data by unknown third parties. This situation can create tension between disclosing and withholding of information (Li et al., 2010). This section identifies user responses from the literature to show how smartphone users can

respond to privacy risks. Beldad et al. (2011) identified three main ways users respond to privacy risks. These are: information seeking, the withholding of information, and the fabrication of information.

3.4.1 Information Seeking

Information seeking refers to the search for relevant information that will resolve the uncertainties surrounding information disclosure (Beldad et al., 2011; Mothersbaugh et al., 2012). The following discusses two main reasons for information seeking:

Information seeking is one response to permission request in the smartphone context (Boateng et al., 2019). For example, permission requests from apps are how developers disclose how apps will interact with the device resources. Discerning users may seek additional information to make informed choices. Although studies suggest that most users do not read privacy notices (Garrison et al., 2012), information seeking is one way for users to resolve disclosure tension and maximise disclosure payoff. Information disclosure involves a trade-off between the perceived costs and benefits of disclosure (Acquisti et al., 2015; Cottrill and Thakuriah, 2015). Therefore, information seeking aims to obtain the relevant information to ensure optimal decision making. For example, using a mobile app often requires sharing personal information for an expected benefit. This involves making an informed decision if the benefit is to be maximised. Therefore, through information seeking, users gather information to engage in risk-benefit analyses, which allow them to make choices that maximise the benefit payoff.

Information seeking addresses vulnerability. Vulnerability refers to the user's perception of insecurity to potential privacy risks. Smartphone users feel vulnerable as they are unaware of unwarranted access to or unauthorised usage of their data (Li et al., 2010; Wang et al., 2016). However, information seeking provides the opportunity for users to develop trust in organisations as they come to know about measures put in place to protect their personal information. Once trust and good reputation have been established through information seeking, users are reassured about informational privacy (Beldad et al., 2011; Capistrano and Chen, 2015).

3.4.2 Withholding of Information

Information withholding refers to the user's refusal to disclose the information requested by data collectors (Beldad et al., 2011). Although the disclosure of certain information is sometimes a condition for using apps (Martin et al., 2016), users do withhold information. This section discusses three main reasons for withholding information:

When information seeking fails to resolve uncertainty. When information seeking fails to resolve uncertainty, information is withheld. As mentioned in 3.4.1, information seeking aims to eliminate the discomfort related to the uncertainties arising from the sharing of personal data. This is because disclosing personal information produces feelings of vulnerability and uncertainty. These perceptions introduce uncertainties related to information seeking. However, information seeking does not always produce a positive outcome. Hence, when the outcome is unsatisfactory, information may still be withheld (Beldad et al., 2011; Wang et al., 2016).

Concerns about ubiquitous connectivity of smartphones. The ubiquitous connectivity of smartphones is another reason users withhold information (Choi, 2016b; Markos et al., 2018), as smartphones allow for multiple connections. These connections, which may include service provider networks, embedded sensors, Wi-Fi, and third-party apps, expose the users to a wide audience. Therefore, the multiple contexts in which data are potentially exchanged trigger privacy risks, resulting in the refusal to disclose (Almuhimedi et al., 2015; Wachter, 2018).

Information is withheld if it is not fit-for-purpose. Information is withheld if it is perceived as not fit-for-purpose. This happens if the perceived privacy risk has a stronger influence than the perceived benefit of disclosure (Keith et al., 2013; Lin et al., 2016). For example, the perceived risk from a new app may result in the withholding of information from similar apps. However, some apps deny users full functionality if the requested information is not provided. Thus, users are caught between the desire to withhold information and using the full functionality of the app.

Studies show that, in such situations, information is either withheld or fabricated (Beldad et al., 2011).

3.4.3 Fabrication of Information

Users fabricate information to resolve the tension between refusal and the desire to use an app. By fabricating information, users conceal personally identifiable information. Some reasons users fabricate information have been identified in the literature. Information is fabricated when perceived benefits and risks of disclosure equalise. When users are unable to strike a balance between the perceived risks and benefits of disclosure, they engage in pseudo-anonymity through fabrication to mask their identity or to limit the data collector's ability to identify them (Osatuyi et al., 2018; Thory, 2016). Information fabrication minimises the privacy concerns of the user but reduces the value of the disclosed information for the collector. Users also fabricate information because of a lack of trust (Bansal et al., 2016; Beldad et al., 2011).

3.5 Smartphone Users' Categories

To effectively address privacy concern surrounding the use of smartphones, researchers have categorised users to understand their different interactions and attributes. Categorising smartphone users enable better understanding of the various ways users experience and respond to privacy threats (Malhotra et al., 2004; Son and Kim, 2008). In order to analyse the complex relationships between privacy influencing factors and user attributes, Son and Kim (2008) recommends the development of relevant user-categories related to information privacy-protective responses (IPPR) so that the outcomes of this complex relationship can be systematically investigated. Furthermore, Son and Kim (2008) argues that patterns emerging from such investigation brings clarity to why there are similarities or differences between types of users and responses. For example, Son and Kim (2008) identified six types of user responses - refusal, misrepresentation, removal, negative word-of-mouth, complaining directly to online companies, and complaining indirectly to third-party organisations. Similarly, Beldad et al. (2011) categorisation of user responses discussed earlier (see section 3.4) resembles Son and Kim (2008) user categories as they both reflect discomfort about inappropriate data collection.

User responses are attributed to the diversity of users (Bhih et al., 2016). Therefore, several types of smartphone users are recorded in the literature (Bhih et al., 2016; Zhao et al., 2016). Falaki et al. (2010) suggests that categorising smartphone users and tailoring privacy support along those lines addresses the error of one-size-fits-all. Otherwise, generalised support will only be marginally useful or benefit a small proportion of users.

3.5.1 Users Characterisation by App Usage and Demography

Falaki et al. (2010) characterised smartphone users into two dimensions according to usage. These are, (1) user interactions and (2) application use. Falaki et al. (2010) found that users differ by one or more characteristics stemming from the purpose of usage. For example, some users are more inclined to gaming or social interaction. According Dinev (2014) and Lee et al (2014) usage characteristics influence the perception of information sensitivity and the willingness to disclose personal information. Accordingly, Beldad (2015) notes that social network users are more inclined to sharing personal information. However, the activity a user performs determines the usage category (Gu et al., 2015; John et al., 2011). Since this could change quickly depending on the situation, Zhao et al. (2016) argues many studies on mobile application usage behaviour have only scratched the surface regarding the kinds of user-categories. Saying that researchers “have not explored the differences in application usage behaviour between groups of users” (2016, p. 499). Without exploring these differences, the simplifying assumption that all smartphone users should be supported the same way may continue (Bhih et al., 2016; Mekovec et al., 2017; Zhao et al., 2016).

Other studies (Furini et al., 2020; Okamoto et al., 2017; Zhao et al., 2017) have characterised smartphone app usage according to demographic attributes such as gender, age, income and vocation. Zhao et al. (2017) found that photography apps are much more used by female users than their male counterparts. Male users prefer sports, cars, and news apps. Similarly, learning-related apps are used more frequently by students than businesspeople who used travel and navigation apps more often. Furthermore, age of users is another aspect of smartphone users’ characterisation (Bhih et al., 2016; Del Rosario et al., 2014). However, most studies

characterised smartphone users according to attributes that are not privacy related. Privacy attributes such as levels of privacy concern is directly related to disclosure decision (Bansal et al., 2010a; Kokolakis, 2015). Confirming this, Pavlou (2011) argues that there is consensus in literature that information privacy concerns reflect information sensitivity. Therefore, relying on a characterisation scheme that is informed by privacy attributes is better for the current study seeking to investigate how and why users perceive information sensitivity differently.

3.5.2 Users Characterisation by Privacy Attributes

Understanding the differences in smartphone users' perceived information sensitivity requires the characterisation of users along privacy attributes (Mekovec et al., 2017; Wisniewski et al., 2017). Including privacy concerns into the analysis that provides insight for tailoring privacy support to users ensures that privacy sensitivities are taking into account (Kumaraguru and Cranor, 2005; Zhuo et al., 2017). This is important because the decision to share personal information is connected to how users perceive privacy risks (Acquisti et al., 2017; Kulyk et al., 2019). Therefore, Mekovec et al. (2017) stressed that researchers should focus on understanding online users' privacy concerns to improve personalised or segmented services. Responding to this call, Wisniewski et al. (2017) characterised users on the Social Network Sites (SNSs) into six based on their privacy management strategies. These are, privacy maximisers, selective sharers, privacy balancers, self-censors, time savers/consumers, and privacy minimalists. Also, Wisniewski et al. (2017) characterised others according to privacy proficiencies on the SNSs, ranging from novices to experts. These characterisations provide the opportunities for supporting users' privacy decisions regarding personal information management (Wisniewski et al., 2017; Zhao et al., 2016).

Hann et al. (2007) characterised online users into three categories by using their rankings of various benefits and concerns related to privacy. These categories are, privacy guardians, information sellers, and convenience seekers. According to Hann et al. (2007), privacy guardians are more sensitive to personal information than information sellers who are willing to provide information in exchange for money. Convenience seekers are willing to exchange information for convenience. However,

privacy analysis that focus on perceived benefits or convenience alone is incomplete because it justifies unwarranted collection and neglect the worrisome aspects of collecting personal data (Martin et al., 2016; Pavlou, 2011).

According to Martin et al. (2016), context changes how different categories of people perceive privacy concern. However, some categories maintain stable privacy concern across contexts, and for others this differs. Privacy is context-driven and influenced by complex perceptions that must be understood. This suggests that understanding how different categories of people perceive privacy concern help organisations respond to privacy concerns with appropriate policies, products, and services.

3.5.3 Alan Westin's privacy characterisation

Alan Westin conducted several privacy-related surveys covering general privacy, consumer privacy, medical privacy, and other privacy-related areas between 1978 and 2004 to characterise people according to their privacy concern level (Kumaraguru and Cranor, 2005). Westin characterised people into, privacy fundamentalists, privacy pragmatists and privacy unconcerned. Privacy fundamentalists value privacy highly and are very inclined to refusing information disclosure. They want strong laws that secure and control how organisations use peoples' personal information. They feel their privacy have been eroded and are strongly resistant to further disclosure of themselves. Conversely, privacy unconcerned usually trust organisations, have no problem with disclosing personal information. Privacy pragmatists normally weigh the benefits of disclosure and of the various opportunities involved against the level of intrusiveness of the personal information sought (Kumaraguru and Cranor, 2005). However, it is unclear how context influences these categories.

Westin based his characterisation on respondents' agreement with three statements: "(1) consumers have lost all control over how personal information is collected and used by companies; (2) most businesses handle the personal information they collect about consumers in a proper and confidential way; and (3) existing laws and organisational practices provide a reasonable level of protection for consumer privacy today" (Kumaraguru and Cranor, 2005, p. 13)

Westins characterisation represents an important scheme for characterising the different levels of privacy concerns among online users (Kumaraguru and Cranor, 2005; Mekovec et al., 2017). Many privacy researchers have used Westin's characterisation to compare their own survey results. (Ackerman et al., 1999; Dolnicar and Jordaan, 2007; Milne and Bahl, 2010; Turow et al., 2009). Studies rely on this characterisation because general privacy concern, as Westin's characterisation is called, represents important personal factor that influence individuals' privacy protection behaviours. Whilst Westin's categorisation require revalidation across contexts, it is a good starting point for the research seeking to understand differences in privacy decisions antecedent such as the perception of information sensitivity. Moreover, the Westin's privacy categories were developed from a very wide survey study that implies good representation of the general public (Kumaraguru and Cranor, 2005). Mekovec et al. (2017) and Wisniewski et al. (2017) suggest that Westin's categorisation can be extended into different contexts to study individual's privacy behaviour. More importantly, Westin's categorisation is widely accepted because it describes how individuals respond to privacy risks pertaining to personal information (Mekovec et al., 2017; Wisniewski et al., 2017).

The factors that influences users' willingness to disclose personal information have different impacts across the Westin's privacy concern categories (Jai and King, 2016). Jai and King (2016) found that the fundamentalist attribute determines how individuals' age influences the willingness to share personal information. For example, younger people shared more personal information with the exception of those who are fundamentalists. This shows that the fundamentalist factor is a privacy protection factor and users in this category prefer to give express consent before personal information can used (Mekovec et al., 2017).

Despite the wide acceptance of the Westin's categorisation, it is criticised for being "pejorative" in describing the privacy fundamentalist by The Electronic Privacy Information Center (EPIC) (Center, 2002). The EPIC argues that the so-called fundamentalists are reasonably concerned about privacy and so they should not be portrayed as extremists. Responding to this, Hann et al. (2007) referred to the group of people with behaviour similar to the privacy fundamentalists as "privacy

guardians", thus confirming the existence of the attribute. Therefore, the privacy fundamentalists will be referred to as privacy guardians in the remainder of the thesis.

According to Mekovec et al. (2017) understanding the relationship between the attributes of privacy guardians, privacy pragmatists, privacy unconcerned and online privacy concerns expands the understanding of the way that attributes influence behaviours differently. From Westin's categorisation emerged the spectrum of personal information protection beliefs, with the privacy guardians at one end of the spectrum, the privacy unconcerned at the other, and the privacy pragmatists in the middle (Kumaraguru and Cranor, 2005). However, Martin et al. (2016) argue that the current state of privacy research fails to capture the full range and richness of the factors that are important to people when they make privacy decisions along this spectrum. Additionally, Acquisti et al. (2015) and Barhamgi et al. (2018) recommends that privacy in the context of the present information age requires a balance between privacy protection and information sharing. This validates the need to understand how users perceive information sensitivity through the interaction of the critical factors.

3.6 Conclusion

This chapter concludes the review of literature for the research that aims to understand how different categories of smartphone users perceive information sensitivity. To understand users' information sensitivity in this context, various insights must be linked. It is important to understand the various ways of collecting data as well as the resultant privacy risks because smartphone use data collection put users' data at risk. Privacy risks determine user responses which differs across privacy concern categories. Several categories characterise smartphone users. However, a modified naming of Westin's privacy categories provides the starting point for the current research. The remainder of this thesis refers to the privacy fundamentalist as the privacy guardian to avoid pejorative naming. User-categories differ in how they perceive information. Therefore, characterising users sheds light on how smartphone users perceive information sensitivity differently. Understanding the differences in perceived information sensitivity provides the insight for tailored privacy. The next chapter discusses the theoretical framework of the research.

Chapter Four

4. Theoretical Framework

4.1 Introduction

Chapters 2 and 3 lays the foundation for understanding privacy and the factors influencing the perception of information sensitivity in the smartphone context. Understanding privacy and perceived information sensitivity contextually set the scene for identifying which factors will be researched. While this background is important, the theoretical framework is relevant for achieving the aim of the research. Theories allow complex ideas to be linked. Therefore, the theoretical framework applied in this research enables the complexities of users' privacy decisions to be structured (Osanloo and Grant, 2016). However, there are many theories that IS researchers have employed to investigate individuals' privacy decisions. Four common ones are discussed to assess their fitness but two (restricted access/limited control and the concept of bounded rationality) will constitute the theoretical framework.

1. Rationality theories (Blau, 1997; Hodgson, 2012).
2. The control theory of privacy (Beardsley, 2017; Fried, 1968; Westin, 1970).
3. Restricted access/limited control- RALC (Tavani, 2007).
4. The concept of bounded rationality (Simon, 1982).

The chapter features five main sections. Section 4.1 provides the introduction and lists the theories discussed. Section 4.2 discusses what is a theory. It expresses the type of theory the current research will develop and how such theory is proposed. Section 4.3 focuses on theoretical framework as a frame of reference for conducting research studies. It points out how theories support research. Section 4.4 discusses privacy theories and privacy decisions which is broken into four subsections focusing on each privacy theory. The subsections assess each theory to determine its fitness for the current research. The final section 4.5 provides the conclusion to the chapter.

4.2 What Is a Theory

A theory is defined as "a statement of relations among concepts within a set of boundary assumptions and constraints" (Bacharach, 1989, p. 496). This definition will guide in proposing a middle-range theory as recommended by Hassan and Lowry (2015). Middle-range theories are logically interconnected and contextual sets of propositions resulting from in-depth specialisation in a specific subject matter. Since the current research investigates nuances in privacy decisions of smartphone user-categories, proposing a middle-range theory is justified. Moreover, this type of theory differs from an all-inclusive effort to explain phenomena across a wider scope in a grand theory such as the concept of bounded rationality and RALC. Middle range theories are useful in explaining contextual phenomenon because they are focused and do not obscure important nuances unlike the overreaching abstraction of grand theories. However, middle range theories contain abstractions that are close to data, thus allowing generalisations (Hassan and Lowry, 2015). A middle range-theory built through the process of induction can be validated in a deductive study because middle range theories suggest hypotheses that could be empirically tested (Corbin and Strauss, 1990; Hassan and Lowry, 2015; Strauss and Corbin, 1998). However, such a deductive testing is outside the scope of the current research. In addition, middle range theories emanate from more nuanced levels of analysis by looking at the attributes of individuals instead of interactions between the individuals. Hassan and Lowry (2015) and Hassan et al. (2019) outlines how middle range theories can be developed:

1. A focus on patterns found in data. To do this, the current research derives the theory from empirical data.
2. Create intermediate concepts and propositions that operate between grand theories and minor working hypotheses.
3. Develop and refine the concepts and propositions by focusing on the specific phenomena regardless of whether the goal is to generalise to groups or to describe individual characteristics. Doing this will allow the current research to focus the propositions on the phenomenon of interest across smartphone user-categories.

4. Evaluate the originality and novelty of the concepts and propositions by exploring alternatives to current ways of thinking about the concepts and the emerging theory.

Theory plays important role in qualitative research (Hassan et al., 2019b). In the current research, the theoretical framework will provide; (1) the basis to determine when the right of privacy is invaded, (2) the basis to link the concepts identified in the field study, (3) the basis for field entry to determine what data to collect and examine, and (4) the structure of the outcomes of the research.

4.3 Theoretical Framework as a Frame of Reference for Conducting Research Studies

Eisenhart (1991) defined a theoretical framework as "a structure that guides research by relying on a formal theory constructed by using an established, coherent explanation of certain phenomena and relationships" (1991, p. 205). Therefore, Osanloo and Grant (2016) argue that theoretical framework serves as the foundation of a study by guiding various aspects of the research. Since the current research problem resides in the privacy and decision-making domain, four privacy and decision-making theories will be considered to justify the selection of the most appropriate ones. The appropriate theories must underpin the research topic and the phenomenon studied. Theories are the researcher's lens with which to make sense of the empirical data as it is the needed frame of reference for conducting the research (Li, 2012). Theories help to strengthen the research argument by making the findings more acceptable (Osanloo and Grant, 2016).

Selecting the appropriate theoretical framework for a research requires a consideration of the research ontology and epistemology because ontology and epistemology intersect theory (Osanloo and Grant, 2016). Furthermore, Osanloo and Grant (2016) suggests that the working knowledge of the theory is required to justify and consider how the theory responds to the research aim and problem. As an interpretivist researcher, my ontology and belief are informed by the interpretivist philosophy (see chapter 5). The interpretivist researcher has a subjective ontology and conceives reality as a product of social interaction from human actions and the social context. This recognition according to Dudovskiy (2016) is a fundamental way

of drawing meanings from the social world. Since theories systematically interconnect ideas (Li, 2012), the theoretical framework is applied by this researcher to draw meanings systematically from the social reality of research participants. Apart from adding structure to a research study, a theoretical framework provides the evidence for comparing research findings when interpreting new data (Osanloo and Grant, 2016).

According to Osanloo and Grant (2016) IS scholars argue that over reliance on theoretical framework in IS studies can hinder creative and innovative research. The concerns pertain to the relationship between theory and empirical data in research. To address these concerns, interpretivist researchers should not confirm or refute theory as positivist studies do. Theoretical framework in interpretivist studies explains relationships among concepts and on how a set of concepts are formed (Hassan and Lowry, 2015; Osanloo and Grant, 2016). This explains why theories are used in interpretivist studies to provide description of the phenomena of interest, to guide analysis of constructs, and to explain how, why, and when things happen (Orlikowski and Baroudi, 1991). Doing this enhances the depth of insight drawn from the research phenomenon through critical probing and comparison with other related phenomena (Dudovskiy, 2016; Silverman, 1998).

It is important to make explicit and theory-based description of the social issues under investigation if the aim of enabling critical understanding of the phenomenon will be realised (Corbetta, 2003; Li, 2012). Therefore, critical conceptualisations of human action should be guided by relevant theories (Osanloo and Grant, 2016). Moreover, theories support the explanation of human interactions and their context through theoretical integration which is the final stage in grounded theory studies. Theoretical integration relates the emerging theory, as an act of collaborative research to other theories in the same or similar field (Urquhart et al. 2010). The process of integrating theory requires uncovering the existing theory or theories guiding the research through the nature of its discourse. Doing so evaluates the novelty of the emerging theory as alternative theoretical strategies could be crafted from the discourse of the study (Hassan et al., 2019a; Urquhart et al., 2009).

4.4 Privacy Theories and Privacy Decisions

Having examined the importance of the theoretical framework in a research study, the following subsections looks at four common theories IS scholars have applied to interpret users' privacy decisions. Therefore, as mentioned in section 4.1, the rationality theories (Blau, 1997; Hodgson, 2012), the control theory of privacy (Beardsley, 2017; Fried, 1968; Westin, 1970), restricted access/limited control theory (Tavani, 2007) and the concept of bounded rationality (Simon, 1982) will be discussed and evaluated with regards to the context and phenomenon of the research.

4.4.1 Rationality Theories and Privacy Decisions

The rational choice theory posits that individuals possess consistent preferences between alternatives. Individuals therefore, choose the utility maximising option, discount future events consistently, and act upon complete information or known probability distributions for all possible events (Hodgson, 2012). Similarly, the privacy calculus theory posits that individuals undertake a calculus (assessment) of the risks and benefits of information disclosure to decide whether to disclose personal information. In performing this calculus, individuals expect at least a balanced outcome and are more likely to disclose personal information when the anticipated benefit is greater (Fife and Orjuela, 2012). This concept assumes that individuals expect economic value or social benefit for losing control of their personal information (Lee et al., 2015).

Rationality theories such as the rational choice theory (Hodgson, 2012), the privacy calculus (Fife and Orjuela, 2012), and the theory of planned behaviour (Ajzen, 1985) assume that people manage their privacy through rational decision making or by making choices that maximises utility. This process assume that individuals' preferences are updated continuously with new information. Rational decision-making process is a deliberative one in which individuals weigh costs and benefits before making decisions that maximise manifest payoffs (Taneja et al., 2014). This suggests that the maximisation of the payoff (mostly through rewards) and service (real satisfaction) is the prime focus of rationality.

There are several rationality theories, with each representing different ideology and its own assumptions about decision making (March, 1978). Theories describing rational decision-making processes have received contributions from disciplines such as mathematics, economics, including areas such as finance, medicine, military, and cybernetics (Oliveira, 2007). Most of these disciplines are areas that focused on the notion of an objective ontology. Thus, it is not surprising that most rationality theories are one-dimensional in explaining the decision process. The underpinning norm makes rational decision-making theories axiomatic and follow specific methodologies for selecting a course of action. Thus, rationality theories assume that decision makers are well informed and will follow a predetermined decision path such as investigating several possible alternatives from different scenarios before making a choice (Hodgson, 2012; Taneja et al., 2014). Therefore, rationality theories consist of rationalistic components indicating how decision makers should decide. However, several psychological elements such as attitudes and attributes influence the decision-making process. Therefore, the complex and dynamic influence of psychological elements associated with decision-making challenges the straight-line decision process of rational theories (Smith et al, 2010).

Applying rationality theories to privacy decisions suggests that individuals could act logically and autonomously in deciding whether to share personal information and keeping their interests in mind through a trade-off between risk and benefit. This trade-off is known as privacy calculus (Hodgson, 2012). The decision process behind this trade-off is thought be conscious and rational. However, rational theories are criticised for making unrealistic assumptions about the rationality of decision-makers (Knijnenburg et al., 2017). Rather than being rational, people's privacy decisions are influenced by various heuristics, such as the perception of sensitivity, privacy-setting and interface of a device, and the phrasing of privacy requests (Acquisti et al., 2017). Hence, privacy decisions follow complex and dynamic path that consists of evolving series of interrelated choices. Therefore, data subjects and data collectors can play a role in shaping the outcome of users' privacy decisions (Beldad et al., 2011; Beldad, 2015; Knijnenburg et al., 2017). This complex process differs from the traditional and structured path assumed by rationality theories. In rational economic theory, for example, the rational decision-making method consists of the following steps: (a) an

analysis of the alternative, (b) evaluating the desirability of the alternative, and (c) choosing the best alternative by combining both desirability and feasibility (Rubinstein, 1998). However, Oliveira (2007) argues that people rarely adhere to logical methods of choice, suggesting that complexities in privacy decisions does not fit the assumption of rationality theories. Adding to the complexity is the fact that peoples' perception differs (Assemi et al., 2018), and the different ways of perceiving privacy risks make standardised prescription of rational decisions inadequate. Therefore, a more nuanced and tailored way of explaining privacy decisions is required (Knijnenburg, 2017). This approach is important because individuals' privacy decisions depend more on cognitions and perceptions than on rational assessments (Taneja et al., 2014; Xu et al., 2011a).

Moreover, malicious practices such as presenting misleading information, may lead an individual to act against their best interest. This suggests that the "best interest" may not always be the outcome of a rational privacy decision process. The concept of "privacy dark strategies" (Bösch et al., 2016) points to this possibility. This is a practice in user-interface design that seeks to manipulate users into disclosing personal information. "Privacy dark strategies" skew privacy decision making because useful information that aids accurate decision making is withheld, thus constraining rationality. The occurrence of these practices indicate that individuals often do not have all the relevant information to support rational privacy decisions.

Without relevant information, privacy decisions' uncertainties are created (Simon, 1982). An appropriate rational response to uncertainty is to make an informed guess about uncertain future consequences and a guess about uncertain future preferences through information seeking and evaluation. Information seeking and evaluation supports informed decision-making process (Beldad et al., 2011; Capistrano and Chen, 2015). However, the challenge with the smartphone small screen size limits reading of lengthy privacy notices and in turn hinders adequate information seeking response. This suggests that rational response in the smartphone context is constrained. Conversely, Kusyanti and Puspa (2018) argue that information seeking is possible through the smartphone interface by continuously scrolling the screen, but most users avoid doing this because it is cumbersome. In addition, malicious use of sensors that overrides users' choice and

consent can nullify the outcome of rational deliberation to withhold information. Thus, smartphones make rational theories not applicable and consequently rational theories do not sufficiently explain or guide the current research.

4.4.2 The Control Theory of Privacy and Privacy Decisions

According to Fried (1968), privacy is the control individuals have over personal information. Similarly, Miller (1972, p. 25) agrees with this version of the control theory by describing privacy as ‘‘the individual’s ability to control the circulation of information relating to him’’. Additionally, Westin (1970, p. 7) endorsed the control theory by arguing that privacy is the ‘‘claim of individuals…to determine for themselves when, how, and to what extent information about them is communicated to others’’. Therefore, the control envisaged by the control theorists seems to relate to control over disclosure. In other words, individual could decide whether to disclose personal information about oneself. Thus, the control theory suggests that privacy is directly linked to one having control over information about oneself (Tavani, 2008). This implies that the control a person has over information about themselves is dependent on the ability to control access to a piece of information. Control could be maintained through different levels of relationships. For example, a person’s friends on Facebook have access to the personal information posted on a personal page as the social network platform allow users to discriminate between friends and other publics, even though the control over the information disclosed to Facebook may be problematic. However, one of the control theory’s main postulation is in recognising the role of individual’s choice in privacy theory (Anderson et al., 2017; Tavani, 2008).

The challenge with the assumption of the control theory is how impracticable it seems for a person to disclose personal information and still retain the privacy of the disclosed information. For example, if A discloses personal information to B, it becomes impracticable for A to control how B uses the information. So, the control A has is the choice to disclose or not to disclose. However, the mechanism of choice and consent (Acquisti, 2004b; Acquisti and Grossklags, 2005) when not circumvented by sensors could be effective in controlling access to information.

Whereas the control theory’s account of informational privacy extends rationality by explaining what the individual can do with their choice, rational theories prescribe

how the choice is made. In other words, rational theories indicate the process or "how" to make a choice and control theory indicates "what" the decision maker could do with his/her choice. A challenge with the control theory is that it does not clearly specify how much control a person should have over information (Tavani, 2008). This suggests that control must be total or absolute over one's personal information for one to have privacy. But ICT has changed such a conception of privacy (Anderson et al., 2017). Apart from the amount and the speed with which personal information can be collected and exchanged, the type of information that can be collected through enabling technologies like the smartphone sensor has also changed individuals' ability to have privacy in the sense of the control theory (Crema et al., 2017; Kulyk et al., 2019).

In the smartphone context, the ability of individuals to control their personal information privacy is a challenge due to the *leakiness and creepiness* in the mobile apps space. *Leakiness and creepiness* refers to the feelings that mobile apps could access and leak personal information without explicit permission (Kulyk et al., 2019; Shklovski et al., 2014). Therefore, the control theory is not sufficient to fully explain or guide the current research that investigates how the privacy perceptions of different categories of smartphone users are shaped by critical factors. Moreover, a theoretical framework should enable the researcher to define and determine when privacy is at risk or minimised, but this cannot be realised using the control theory (Osanloo and Grant, 2016).

Privacy perception differs with types of information and context. Smartphone users apply privacy control selectively over types of information across different context. For example, privacy perception differs in social media and business apps (Armando et al., 2015). Since the control theory does not clarify the varying privacy perceptions, it does not capture the reality of the smartphone user (Armando et al., 2015; Kulyk et al., 2019). To address the limitations of the control theory, Tavani (2007) postulated the Restricted Access/Limited Control (RALC) theory of privacy.

4.4.3 Restricted Access/Limited Control (RALC) and Privacy Decisions

The main insight from the RALC theory (Tavani 2007) is that a person has privacy if his/her information is restricted from intrusion and unauthorised access by others. RALC differentiates between privacy and the management of privacy. Restricted access is required for one to have privacy. Privacy can be managed by allowing individuals to limit the access others have to their personal information. This implies that privacy can be managed by a permission model.

Like the control theory, the RALC indicates the role that individuals' control plays in privacy theory. However, unlike the control theory, RALC does not require individuals to have absolute control over their personal information to have privacy. Rather, only limited controls are needed to manage one's privacy (Tavani, 2008). Therefore, Tavani (2007) argues that privacy is preserved when access to information is restricted to the right people or systems. To achieve this, people create "privacy zone" as instrument of control that enables them to decide which information should stay private. Similarly, the communication privacy management (CPM) theory advocates boundary formation to guide the disclosure of personal information and to determine the most effective privacy protection strategies (Petronio, 2002). Although, "privacy zones" and privacy boundaries could be violated and personal information are collected surreptitiously, the creation of privacy zone is nonetheless an effective means of managing privacy.

The "privacy zone" and other constructs recommended by RALC provides useful starting points for this search as the RALC have been widely used by IS researchers (Beldad et al., 2011; Smith et al., 2011). An example of the "privacy zone" in the smartphone context is where a mobile navigation app is allowed access to a user's location data but not to contact information. However, such levels of access could even be more selective. The selective granting of access to information explains the notion of restricting and selective access that individuals use to manage privacy. Hence, it is important to keep information that is rightly accessed in the context of disclosure otherwise, the contextual integrity of the information is breached and the intention of restricting access and limiting control would be defeated. In this sense, Nissembaum (2004) theory of contextual integrity can be incorporated into the RALC. Whereas Nissembaum emphasises context as determinant of restrictions, RALC

emphasise the nature of information as the determinant of privacy protection (Tavani, 2008). The two concepts are compatible because the nature of information often determine its contextual restrictions. For example, users of the new NHS COVID19 track and trace app have an expectation that health status information disclosed in the app should remain strictly within the NHS which is the context of disclosure (Guinchard, 2020).

The RALC advocates the implementation of privacy notices through its publicity principle mechanism to aid the control of privacy. The publicity principle states that "rules and conditions governing private situations should be clear and known to the persons affected by them" (Tavani, 2007, p. 32). Rules and conditions governing privacy are often presented in form of privacy notices (Tavani, 2008). However, studies (Angulo et al., 2012; Capistrano and Chen, 2015) shows that most smartphone users do not read privacy notices, therefore, they are not well informed about privacy options. To address this, Angulo et al. (2012) and Schaub et al. (2017) advocates for more usable privacy notices to support informed privacy decisions in the smartphone context.

Privacy notice provides information that should guide informed privacy decisions (Schaub et al., 2017). Therefore, the RALC theory provides mechanisms for exercising choice and consent which are important tools for managing privacy. However, regarding the mechanisms of choice and consent, one might ask how the RALC theory can provide insight regarding how different categories of people will exercise choice and consent in a privacy preserving environment? Addressing this question requires privacy concern analysis to differentiate perceived information sensitivities by comparing the responses from different groups of people (Bansal et al., 2016; Kumaraguru and Cranor, 2005). This explains why the empirical investigation in chapter six looks at different groups of smartphone users. Doing this could make the RALC more applicable and tailored to different user groups (Angulo et al., 2012; Balebako et al., 2011). Therefore, it is possible for the RALC framework to inform the design of a new kind of nuanced tailored privacy that respects different individuals' preferences.

Although the RALC has important constructs that can guide this research, the RALC alone cannot fully support the analysis and interpretation of data in the current research. Moreover, even when people read privacy notices, cognitive limitation constrains their understanding (Acquisti and Grossklags, 2005; Simon, 1982). Several constraints known as bounds of rationality have been highlighted in the concept of bounded rationality which will be considered.

4.4.4 The concept of bounded rationality and privacy decisions

Making a rational choice requires a "guess about uncertain future consequences …" (March, 1978, p. 587). However, the way rationality theory deals with this guess has been organised into conceptions of bounded rationality. The concept of bounded rationality refers to rationality constrained or "bounded" by cognition, incomplete information, and time constraints. This concept features prominently in behavioural economics and is concerned with how decisions are influenced by the process of making them (Simon, 1982). In the privacy context, it refers to how the bounds of rationality constrain a subject from fully understanding the consequences of sharing valuable information in an irreversible trade-off (Acquisti et al., 2015; Acquisti and Grossklags, 2005); irreversible because personal information made public can never be made private again.

Incomplete information impedes privacy decision making by limiting a full understanding of the disclosure risks, resulting in inaccurate evaluations. Such situations create uncertainties, with complexities such as context dependencies (environmental influence and timing) adding to them. Apart from this, individuals are constrained by cognitive limitation which suggests that individuals are unable to process and act optimally on large amounts of information (Acquisti et al., 2015). Therefore, individuals who intend to make rational choices are "bound" to make satisficing (rather than maximising or optimising) choices in complex situations (Osatuyi et al., 2018). In the privacy context, individuals deal with cognitive constraints by minimising the uncertainties related to disclosure. They reduce their level of privacy concern by choosing what is "good enough" when the search for alternatives will require more cognitive resources (Spiegel and Silva, 2018). Furthermore, the notion of time constraints assumes that there is not enough time to

gather and evaluate all the available information. As a result, privacy decisions are made from incomplete information (Acquisti and Grossklags 2005) and thus deviates from full rationality (Acquisti et al., 2015; Taneja et al., 2014).

The underlying argument cutting across the various bounds of rationality is that full rationality is bound during privacy decision making. Therefore, bounded rationality results in people sharing personal information without being fully aware of the risks involved in the disclosure (Acquisti and Grossklags 2004). The notion of bounded rationality captures the behaviour of most smartphone users as evidence shows that users share personal information without realising how the information shared are used (Almuhimedi et al., 2015; Ketelaar and van Balen, 2018). Moreover, users are constrained by the presentation layer of the smartphone architecture and task environment which further bound rationality (Jokinen, 2017). One may ask, how can the problems arising from the "bounds" of rationality be resolved or minimised effectively in order to support users' privacy decision making in ways that are tailored to user-characteristics and the decision-making context? In seeking to address this problem, the current research includes the bounds of rationality in the analysis and interpretation of empirical data. In doing this, evidence of the bounds of rationality in the empirical data will be identified in order to seek for ways of minimising its impact. Moreover, the empirical data is categorised along user privacy categories, so it is possible to see how the bounds of rationality operates across the user-categories from which nuanced solutions can be proposed. Therefore, the concept of bounded rationality and RALC theories jointly provides the theorical framework in the current research. Moreover, these theories are often used by information system and interpretivist researchers (Pavlou, 2011). For example, Jens et al. (2014) applied bounded rationality as a theoretical framework to explore how constraints posed by the theory impact on decision making through an inductive and interpretivist study.

The relevant components of the chosen theories are highlighted in table 4.1 below. These components provide theoretical sensitivity for the coding of empirical data as well as helping to structure the empirical data analysis (see chapter six).

Table 4.1 presents the relevant components of the selected theories

Bounded Rationality	**Impact**
Incomplete information	Limits awareness of privacy risks
Time constraints	Limits the reading of lengthy privacy notices
Cognitive limitation	Limits the understanding of disclosure implications
RALC	**Impact**
Publicity rule	Creates awareness of risk and benefits of disclosure
Creation of privacy zones	Assigns levels of sensitivity to types of information
Mechanism of choice and consent	Enables selective access to personal information

Figure 4.1 below illustrates the relationship between the chosen theories and how they are applied in this research. It illustrates that when users are exposed to privacy risks, the resultant privacy decisions they make is impacted by bounded rationality. This in turn determines the privacy mitigation action. Privacy mitigation usually results in applying constructs from the RALC. The arrows show the cause-and-effect relationship. This connection is further explained in chapter seven where empirical data have been integrated into the framework.

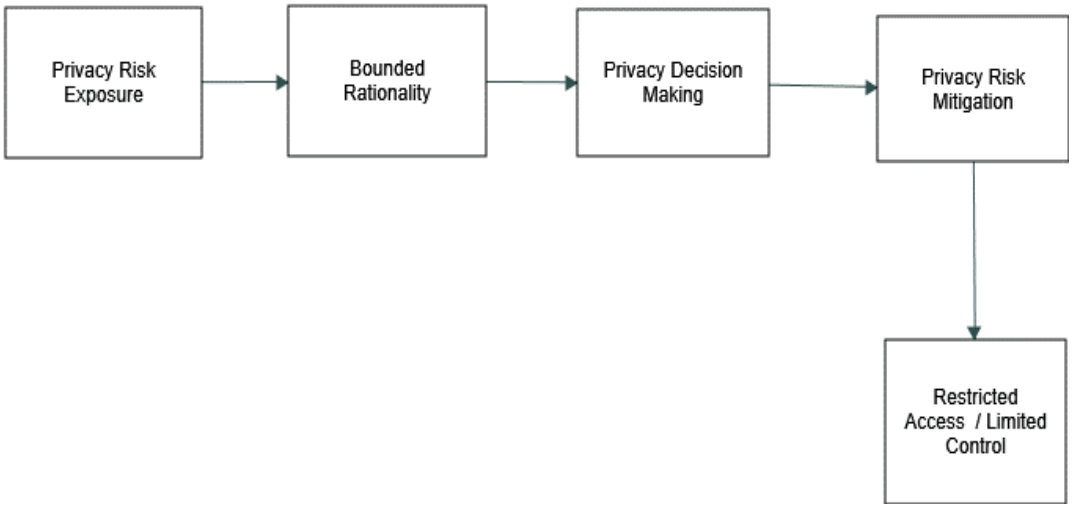

Figure 4.1: Illustrates the relationships in the theoretical framework.

4.5 Conclusion

This chapter provides a detailed overview of the theoretical framework for this research study. It presents a careful consideration of four privacy theories used in Information Systems research with the intent to select the most suitable theoretical framework for the study. A theoretical framework is important in the research because it guides the structure of the empirical data analysis and provides a foundation for knowledge construction throughout the thesis. The concept of bounded rationality and RALC theories have been presented and justified as the theoretical frameworks for this study. This is because they adequately explain and provide the needed guide for data analysis and interpretation. The study uses the mechanisms of choice and consent and the publicity principle of the RALC theory as well as the three bounds of rationality in the concept of bounded rationality as key components. These components inform the wording of interview questions, concept development in the coding, analysis, and interpretation of empirical data. Additionally, the chosen theories are consistent with the underlying assumption of the research philosophy and the grounded theory method. The next chapter presents the detailed methodology applied in this study

Chapter Five

5. Research Methodology

5.1 Introduction

The present research is an empirical study aimed at understanding the differences in perceived information sensitivity among smartphone users. Understanding how users perceive information provides insight for tailored privacy. In doing this, philosophical approaches are evaluated with the research questions in mind. The research questions are the interrogative elements that a researcher uses to investigate the phenomenon of interest (Creswell, 2003). Hence, the appropriate research methodology should be chosen, because methodology is the means of acquiring knowledge about the world (Denzin and Lincoln, 2000). Accordingly, this chapter discusses the methodology and the philosophical paradigms (how knowledge is gained) that is used by IS and social science researchers. In addition, the specific tools used for data collection are discussed. Finally, the approach which the research and researcher will adopt is also explained and justified.

5.2 Philosophical Paradigms

This section discusses three main philosophical paradigms used in information system research (Rahi, 2017). They are positivism, interpretivism and critical research. Pragmatism is not discussed because it is the combination of the positivist and interpretive paradigms. Moreover, pragmatism is closely linked to design science that aims to develop new artefacts or technological solutions. (Rahi, 2017). Paradigms are laws, theories and instruments of coherent and scientific research (Anand et al., 2020). Paradigms are “a set of shared assumptions or ways of thinking about some aspect of the world” (Oates 2006, p.282). In other words, paradigm reflects a basic belief system that is informed by ontology and epistemology (Anand et al., 2020). Philosophical paradigms prescribe the methodology for a scientific inquiry (Guba and Lincoln, 1994; Oates, 2006).

Orlikowski and Baroudi (1991) argue that research paradigms should be employed in information systems research to enrich understanding of behavioural information systems phenomena. To achieve this goal, Orlikowski and Baroudi (1991)

recommends the adoption of the interpretivist and the critical research paradigms by behavioural information systems researchers. The IS researchers' philosophical approach articulates the sets of beliefs that is adopted towards the world and their work (Anand et al., 2020). A paradigm reveals the researchers' ontology (theory of reality), epistemology (theory of knowledge) and methodology (theory of method). According to Chua (1986), the following perspectives distinguish information system researchers.

(i) **Beliefs about the phenomenon or "object" of study.** The belief about the phenomenon or object of study is essentially ontological. That is, a researcher may see the empirical world as objective and independent of human actions or see it as subjective and existing only through the action of humans that creates and recreates it. Additionally, social interactions can be viewed as stable and orderly or as primarily dynamic and conflictual. Regarding this research, the subjective ontology is most suitable because the phenomenon under study is socially and subjectively created (Oates, 2006; Orlikowski and Baroudi, 1991).

(ii) **Beliefs about the notion of knowledge.** This belief represents the epistemological assumptions guiding a study, by which knowledge may be constructed and evaluated. For example, the positivist researcher assumes knowledge is valid only if its quantifiable (Orlikowski and Baroudi, 1991). Such assumption prescribes appropriate research methods and techniques for gathering valid empirical evidence. Hence, positivists believe that large-scale sample surveys and controlled experiments are appropriate research methods because they enable better generalisation. Regarding this research, the qualitative approach is most suitable because it allows deep understanding of subjective meaning of things to be unearthed (Orlikowski and Baroudi, 1991).

(iii) **Beliefs about the relationship between knowledge and the empirical world.** These beliefs are about the role of theory and the methodology that allows the researcher to study the empirical world. The decision about theory

and methodology is influenced by what researchers intend to achieve with a research study. For example, some researchers seek to confirm theories as the means of providing solutions to specialised problems. Others use theories as a guide to understanding social relationships and attributes of individuals (Orlikowski and Baroudi, 1991). Regarding this research, using theories as a guide is most suitable because qualitative studies should not seek to confirm theories. Rather, theories are used to induct new understanding about a phenomenon in qualitative studies (Orlikowski and Baroudi, 1991).

A researcher's position on these three sets of beliefs is the distinctive research perspective or paradigm that an information system researcher adopts (Orlikowski and Baroudi, 1991). Consequently, the paradigms in this chapter are discussed from researchers' beliefs on the ontology, epistemology and methodology of a research (Davies et al., 2018). IS could be studied from the lenses of either the positivist, interpretivist, critical research, or the pragmatist paradigm. However, the phenomenon under study and the purpose of the research determines the paradigm to adopt (Orlikowski and Baroudi, 1991). How information technology (IT) is developed and used in the society is the main preoccupation of IS (Oates 2006). The integral components of IT are people, procedures, data, software, and the hardware used to collect and analyse digital information (Oates, 2006). However, the people component of IT is what allows society to make sense of, and improve IT. Therefore, studying human interaction with IT and how to improve privacy in the smartphone context is the main purpose for this research. This is important because what is known about IT is not only what is produced, but what is understood and reinforced by humans through their action and interaction (Orlikowski and Baroudi, 1991). Therefore, three behavioural science paradigms- positivism, interpretivism, and critical research are considered (Chua 1986).

Positivist studies look at fixed relationships within the phenomena through structured instruments that primarily test theories. Conversely, interpretive studies adopt a nondeterministic view and seeks to explore the phenomena of interest without imposing any predetermined understanding on it. Similarly, critical studies aim to

explore in order to expose inherent structural problems. It critiques the status quo to remove contradictions so that organisations and society can change (Guba and Lincoln, 1994; Oates, 2006; Orlikowski and Baroudi, 1991). Critical studies are usually concerned with evaluation, description and explanation of phenomenon (Orlikowski and Baroudi, 1991). These paradigms will be discussed in more detail and evaluated for fitness to the aim of this research.

5.2.1 Positivism

Ontologically, the positivist view of the nature of reality is objective, external and independent of the social actors (Anand et al., 2020; Davies et al., 2018). According to Lincoln & Guba (1985) positivism is premised on the following notions:

a) There is a single, tangible and fragmentable phenomenon of interest that is uniquely described.

b) There is an independent relationship between the researcher and the object of inquiry. Therefore, a demarcation between observation, reports and theory is required.

c) Generalisations are not necessarily dependent on time and context, implying that scientific concepts are precise with invariant meanings.

d) Cause and effect relationship in a research are one-directional and can be identified and tested through hypothetic-deduction and analysis.

e) The inquiry is thought to be value-free. Implying that there are no influences of human values in the research process and outcome. However, the idea of a value-free research is contested in social sciences (Tsui, 2016). For example, when a research is bereft of human values, it may become unethical and thus cannot be classified as responsible research (Aicardi et al., 2018; Stahl and Wright, 2018).

The positivist researcher uses quantification to generate knowledge about the phenomena to produce measurable, tangible and objective results (Babbie, 2007; Creswell, 2003). Creswell and Poth (2018) argues that positivists approach inquiry this way because of their ontological viewpoint.

Epistemologically, positivists' (empiricists) use empirical and testable measurements to verify or falsify hypotheses or theories through the hypothetic deductive approach (Stahl 2007). The positivist researcher studies social reality by utilising conceptual framework through the techniques of observation and measurement (Corbetta, 2003). Positivists consider reality as an objective construct produced by the direct and one-dimensional relationship between the existing world and peoples' attitudes.

Positivism might be workable in this research by enabling an investigation across a large sample size through quantitative surveys. Doing this minimises contact with respondents and thus researcher's influence on respondents is reduced. Large scale studies enhance credible generalisation (Guba and Lincoln, 1994). However, positivism will not be adopted in this research as pointed out in the following subsection.

5.2.1.1 Criticism of the positivist paradigm

The positivist paradigm is criticised for not understanding human actions (Doolin 1998) because it does not consider the multiple dimensions of influences in the social context, such as culture and politics (Guba and Lincoln, 1994). Therefore, using this paradigm could produce an incomplete picture of the IS phenomenon studied (Orlikowski and Baroudi, 1991). The phenomenon under study is socially constructed and influenced by the smartphone user's perception and context. Perceptions produces different interpretations based on underlying preferences (Furini et al., 2020). Therefore, studying a socially constructed phenomenon that can produce differing and subjective interpretations does not accurately fit positivism (Oates, 2006).

Throughout the 20th century, the positivist paradigm was continually revised in attempts to overcome its criticisms. Post-positivism results from these criticisms and recognises that we cannot be "positive" about the claim of knowledge when studying the behaviour and actions of humans (Oates, 2006). This idea was advanced by writers like Comte, Mill, Durkheim, and Newton (Dudovskiy, 2016). Despite the revision, positivism remains deterministic and assumes that outcomes are determined by causes. Thus, the problem studied by the positivist reflects the need to investigate causes that influence outcomes by reducing ideas into discreet

variables for numerical testing (Crotty 1998; Creswell 2003). The deterministic approach means that positivist/postpositivist paradigm cannot be effectively applied to human studies as it is applied to natural science (Dudovskiy, 2016; Ritchie et al., 2014). This implies that research about people and society should be conducted along alternative pathways to safeguard the intrinsic individuality of human beings (Corbetta, 2003). This is why Dilthey (1883) draws a distinction between natural and human sciences by arguing that knowledge takes the form of explanation (cause and effect) in natural science, while in human science, knowledge comes through comprehension (understanding). Accordingly, the current research seeks to understand human actions.

To summarise, the critique of positivism are as follows. First, experience is considered as a valid source of knowledge in positivism. However, several important concepts such as space, cause and time are not based on experience (Orlikowski and Baroudi, 1991). Second, positivism assumes that all types of processes can be perceived. This is not always possible as some variations of actions of individuals or relationships between individuals can only be narrated by the actors (Dudovskiy, 2016). Corbetta (2003) emphasised this point by saying:

> *While observation is the most direct and immediate way of studying openly manifested behaviours, the only way we can explore motivations, attitudes, beliefs, feelings, perceptions and expectations is by asking (Corbetta, 2003, p. 117).*

Third, positivist studies generally rely on the status quo. In other words, research findings in positivist studies are descriptive, thus they lack insight into in-depth issues like interpretivist studies (Crowther and Lancaster, 2008; Dudovskiy, 2016). However, the positivist/postpositivist paradigms are strong in developing predictive models unlike interpretivism (Guba and Lincoln, 1994). The next subsection evaluates interpretivism regarding its fitness for this research.

5.2.2 Interpretivism

The Interpretive paradigm is increasingly gaining acceptance in the field of IS (Dudovskiy, 2016; Orlikowski and Baroudi, 1991). The main distinction between the interpretivist and positivist paradigm is ontology. The interpretivist believes that

reality is subjective and as a result, our knowledge of reality is a social product that cannot be understood independent of the social actors (including the researchers) that constructs and make sense of that reality (Dudovskiy, 2016; Hammersley, 1992). Therefore, Burrell and Morgan (1979, p. 253) argue that reality is not only a fixed object, but includes "... an emergent social process that is an extension of human consciousness and subjective experience". Therefore, reality cannot be simply observed, rather it can only be “interpreted”. That is why this researcher seeks to explain the meanings that subjects ascribe to their own actions and interactions. However, interpretive researchers share with the positivist the belief that interactions with research participants should be structured to enable orderly transfer and interpretation of meanings as they are formed (Dudovskiy, 2016). Meanings are formed by several influential factors such as context, attributes and attitudes (Bansal et al., 2016; Zhao et al., 2017). Therefore, interpretations of reality could change with time as context and its components change. Hence, interpretive philosophy fits an evolving social phenomenon. Interpretivism in IS research is concerned with understanding the social context of an information system and the social process from which it is developed and constructed by people (Oates 2006). This suggests that people create and assign subjective and intersubjective meanings through interactions with their world (Orlikowski and Baroudi, 1991). Therefore, interpretive research rejects the objective description of events and situations, seeking instead a subjective and shared perception of phenomena (Dudovskiy, 2016).

Generalising to a population is not the main goal of interpretivism (Oates, 2006). Rather, the main aim is to obtain a deep understanding of the phenomena and such understanding can be inferred into other contexts (Woo et al., 2017). Interpretive researchers aim at understanding how and why research subjects interpret and understand events and concepts that influences individuals’ behaviour (Kaplan and Duchon, 1988).

Epistemologically, the interpretive researcher explores and studies people and the contextual interactions that form the perception of their world through a social process (Oates 2006). This " ... social process is not captured in hypothetical deductions, covariances, and degrees of freedom. [Rather] understanding the social process involves getting into the world of those generating it" (Rosen, 1991, p. 8).

This implies that the researcher is immersed in the world of the participants (Oates, 2006; Orlikowski and Baroudi, 1991).

5.2.2.1 Criticism of interpretivist research

The criticisms of interpretive research include the following. First, critics say that interpretive research outcome cannot be generalised because primary data from interpretivist research are profoundly skewed by the personal views and values of research participants (Davies et al., 2018; Hammersley, 1992). As a result, the reliability and representativeness of data is weakened to some extent. To overcome this, Orlikowski and Baroudi (1991) contend that the researcher should describe the context of the sample sufficiently to enable other researchers decide if the research findings could be applied to their context. According to Orlikowski and Baroudi (1991), it is the reader of the research that should generalise and not the researcher. However, data impacted with depth of personal viewpoints and values can provide high level of validity because it tends to be trustworthy and honest (Dudovskiy, 2016).

Second, interpretivist research is criticised for the subjective nature of its approach due to the level of researchers' involvement. Critics say that such level of involvement create room for researcher-bias (Orlikowski and Baroudi 1991). To overcome this shortcoming, interpretive researchers should construct interpretations or explanations that considers the way that subjective meanings are created and sustained in a setting (Anand et al., 2020; Dudovskiy, 2016). In other words, explanations are based on the context from which responses were generated. Such explanations should result in objectivity by revealing causal relationships between concepts, incidences, and context but not in the positivists' one-directional sense. In doing this, interpretivist researchers posit circular and interacting models of causality that provides insight about actors' perception of their social world (Orlikowski and Baroudi 1991).

Third, critics argue that interpretivism fails to explain historical change and how a social order is likely to change over time (Orlikowski and Baroudi 1991). Refuting this criticism, Gibson (1987) argue that interpretivist research reveals underlying connection between social realities that captures complex and time-dependent social phenomenon. By revealing these underlying connections between phenomena, it is

possible see how a social order may change over time (Dudovskiy, 2016; Oates, 2006).

Finally, positivists say interpretive research is largely anecdotal, biased and not systematic (Oates 2006; Orlikowski and Baroudi 1991).

Despite these criticisms, this researcher will use the interpretive paradigm because the paradigm fits the aim of the research. The research focuses on understanding aspects of social reality from the perspectives of the actors that shapes it. This explains why the research investigates the perceived information sensitivity of different categories of users arising from smartphone-use data collection. This investigation is better conducted by speaking to the people involved.

5.2.3 Critical Research

The main contrast with critical research and other paradigms is the evaluative dimension of critical research (Chua, 1986; De Cleen et al., 2018). Unlike the positivist or the interpretive research philosophies, the critical researcher seeks to critically evaluate the social reality investigated. In doing this, critical studies expose what it believes to be deep-seated, structural contradictions in the social systems, and aiming to change the alienating and restrictive social conditions (Davies et al., 2018; Myers and Avison, 2002). Whereas the earlier two focuses on predicting or explaining the status quo, critical researchers believe that the existing and alienating social systems are historically biased and thus seeks to advance grounds that triggers the replacement of the current social systems with non-alienating structures and norms (Davies et al., 2018; Falconer and Mackay, 1999).

Ontologically, critical researchers view reality as historically constituted by human actions that can change when human beings understand the unfulfilling conditions existing in any state of being (Anand et al., 2020; Chua, 1986). In addition, Anand et al. (2020) argue that change in any state of existence is constrained by prevailing systems of cultural, political, and economic domination that hinders peoples' potentials. Therefore, the main goal of critical researchers is to arouse the awareness of the social domination inherent in the social system under investigation in order to empower people to change it (Orlikowski and Baroudi 1991). This implies that critical research paradigm is the philosophy of empowerment and human emancipation in

society. To achieve the goal of empowerment, critical researchers focus on studying every aspect of society where conflict exist, irrespective of the elements that shapes the conflict (Orlikowski and Baroudi 1991). Hence, critical research aims beyond mere technological and managerial efficiency and control (Cecez-Kecmanovic 2001; Oates 2006). Implying that technical solutions and management efficiency must be driven by social change for the wholistic advancement of society.

Epistemologically, critical researchers believe that knowledge emanates from historical practices (Orlikowski and Baroudi 1991). Therefore, the researchers conduct long-term ethnographic and historical studies of structures and processes. Critical researchers assume that the best way to understand a phenomenon is through a historical analysis of "... what it has been, what it is becoming, and what it is not" (Chua, 1986, p. 621) in order to reveal existing conditions and power structures in society (Orlikowski and Baroudi 1991). Therefore, in practice, the critical researcher does not only study and theorise, but is also active in effecting change in the phenomena investigated. Thus, the critical researcher plays a critical role through the research process to motivate change in the status quo (Orlikowski and Baroudi 1991). According to De Cleen et al. (2018), change is possible by creating engagement that will transform various forms of domination and control.

5.2.3.1 Criticism of critical research

Critical research is criticised for lack of clear standard for conducting theoretical evaluation. “What is acceptable theory or explanation is still debatable” (Chua 1986, p.626). This is why critical researchers vary in the approaches used, thus making the research outcome uncertain. This lack of consensus on research approach results in developing research that is easily dismissed as unfair (Alvesson and Deetz, 2000). Additionally, Alvesson and Deetz (2000) suggest that there is overemphasis on conceptual work instead of strong emphasis on empirical work among critical researchers. Orlikowski and Baroudi (1991) noted that critical researchers do not critique their own work, thus they are not reflexive. The lack of reflection on their work implies that they are less critical of their own concepts. This makes them deterministic in their beliefs and assumptions (Orlikowski and Baroudi 1991).

The critical research will not be used in this research because the research aim is not to change the social status quo, but to understand difference in perceived information sensitivity regarding smartphone use data collection. To achieve this aim, this researcher seeks to uncover users' perception of information sensitivity by searching for a deep understanding of users' privacy concerns. Therefore, the interpretivist paradigm is chosen for this study. The next section provides the rationale for this choice and Table 5.1 presents the comparison of the three paradigms discussed above.

Table 5.1 Comparison of the three paradigms discussed.

	Positivist	**Interpretivist**	**Critical Research**
Ontology	"Naive Realism" in which reality is supposed to exist and shaped by immutable natural laws. Testing theories is the only way of obtaining true reality.	Relativist: humans produce and reinforce the social world through their action and interaction.	Historical realist: historical accounts of human constitute social reality in organisations, and societies are this are not static
Epistemology	Rigorous empirical testing verifies hypothesis. Universal laws are searched for Explanations and predictions are tightly coupled and controlled.	The social world is understood from participants' perspectives by interpreting actions. Researchers require prior knowledge to aid the investigations	Knowledge is found in social and historical actions. Critical evaluations generate and evaluate knowledge of social systems.
Relationship between theory and practice	Universal laws governing the external world can be discovered	Generative mechanisms found in social science phenomena should be seen as 'tendencies' explaining the past data but not completely predicting future	Generalisation point to what is regular and not cross-sectional differences. Every aspect of social relationship can be generalised.

		situations.	Data collection must depend on theory to prove or disprove the theory.
The role of a researcher	Should completely be an objective observer, and value-free approach	To engage and interact with research participants and thus perceptions of both parties are changed.	Transforms social relations by initiating change that eliminates social domination.

5.3 The Rationale of Adopting Interpretivism for this Research

Having discussed and evaluated the three paradigms in the previous sections, the interpretivist paradigm is considered suitable for the current research. Interpretivism is well aligned with the theoretical framework that will guide this research (see chapter four subsections 4.4.3 and 4.4.4). For example, Jens et al. (2014) applied bounded rationality to study how constraints posed by the theory impact on decision making in an interpretivist study. Furthermore, the interpretive paradigm is compatible with the research questions outlined in Chapter one. Interpretivism answers ontological questions that view reality as socially construct by human beings through their interactions with each other (Lincoln and Guba, 1994; Oates, 2006). Hence the meanings ascribed to reality is socially constructed (Oates, 2006). Therefore, meanings are captured from the social interaction that develops (Wilson, 1970). Consequently, in attempting to understand meanings in this research, the interpretivist paradigm is considered useful. Current knowledge and beliefs about the phenomena are explored from the perspectives of the participants. This approach aligns with interpretive research (Dudovskiy, 2016; Wilson, 1970).

As already mentioned, the study seeks to investigate the influence of the critical factors on the perception of information sensitivity among smartphone users based on their characterised privacy concern categories. Other issues impacting on privacy

decisions such as smartphone-use data collection and how this influences users' disclosure are also explored. Research questions that aim to understand such complex privacy decision-making process (Beldad et al., 2011) require interpretivism that is designed for capturing complex and active social phenomenon that are context and time dependent (Orlikowski and Baroudi, 1991). Applying the research questions through the interpretivist lens allows this complex phenomenon to be interrogated for relevant meanings (Bryman, 2007; Bryman and Bell, 2015). Moreover, the perceptions and experiences of different categories of users and how they negotiate through various influencing factors should be understood in order to answer the research questions accurately.

Perceptions about a phenomenon is better revealed by the actors that perceives it (Assemi et al., 2018; Xu et al., 2011a). Therefore, in the current research, knowledge is formed based on findings from perceptions that are captured and analysed from the empirical data as well as from extant literature. The empirical data is appropriately gathered by using in-depth interviews to answer the research questions. Therefore, an inductive research process is followed which is discussed next.

5.3.1 Research Approach

The research approach followed in this study is inductive qualitative research. This approach allows the researcher to be immersed in data to develop an understanding of the ways the phenomenon is socially constructed (Woo et al., 2017). Induction enables accurate interpretation of participants' social world by allowing alternative explanation of issues. In this way and unlike deduction, the process of inducting meanings from data is flexible (Jebb et al., 2017; Woo et al., 2017). Flexibility allows the researcher to follow new leads emanating from data such as the process of theoretical sampling in GT (Glaser and Strauss, 2009). Gioia et al. (2013) suggests that inductive approach fits qualitative data collection by allowing an iterative data collection that throws light on hidden aspects of the phenomena of interest. Woo et al. (2017) recommends the following as best practices for conducting inductive research:

- A clear purpose: the purpose of the research should be stated in the research motivation and guided through the research questions. The purpose directs the methodology and data gathering.
- Explore the data: the researcher should search through the data in all possible ways to detect hidden phenomena that can lead to theory development.
- Flexibility in data analysis: the researcher can come up with novel ways data can be viewed. In this way, the chances of finding surprising and intriguing patterns in data is increased. Flexibility implies that a data set can be used for multiple analytic purposes leading to further probing of the phenomenon of interest in greater depth. Flexibility in data analysis is important because patterns in the data are not always linear, so multiple insights can emerge from a single pattern.
- Cross-validate findings: the researcher should cross-validate research findings by comparing discoveries and patterns in the data with prior literature.

The choice of interpretivism and inductive research approach requires appropriate methods for gathering knowledge (Bryman and Bell, 2015). Therefore, the next section discusses the research methods used by interpretivist researchers in capturing the social reality they investigate.

5.4 Research Methods

As discussed in the previous section, the choice of philosophical paradigm in a research influences the choice of methods that the researcher uses to collect data (Bryman and Bell, 2015; Creswell and Poth, 2018). Hence, the following sections will discuss the options for obtaining data. The researcher's choice of method is also influenced by the kind of things studied such as the natural world or human subjects. This research studies human subjects and explores perceptions towards information sensitivity. As the interpretivist paradigm was considered suitable, the methods compatible with the interpretivist paradigm will be considered.

IS researchers commonly use methods such as experiments, survey, design and creation, case study, action research, ethnography, and grounded theory in their studies (Denscombe 2003; Oates 2006). However, some of these methods are not

relevant to the present study. For example, the interpretive design and creation method is applicable to studies focusing on the development of IT product such as an artefact (Oates 2006), and this is not the goal of the present study, therefore, it will not be discussed. Additionally, the interpretive experiment method is not appropriate for the nature of the present study. An experiment aims to prove or disprove causality between variables in order to establish cause and effect relationship (Bryman and Bell, 2015). The interpretive research methods discussed are, ethnography, case studies, action research and grounded theory (Falconer and Mackay, 1999; Oates, 2006). The most popular methods of primary data collection in interpretivist studies are interviews and observations (Chirban, 1996; Jamshed, 2014), hence they are also discussed.

5.4.1 Ethnography

Ethnography is a method often used in socio-cultural studies that involves the prolonged observation of a group, typically through participant observation (Bryman and Bell, 2015). Usually, researchers gather data by being immersed in the culture of the people or through separate interviews with members of the group (Creswell, 1998). According to Myer (1997), ethnography emanates from social and cultural anthropology, hence ethnographers spend significant amount of time with research participants to allow for immersion into the culture and lives of the people being studied (Lewis, 1985). In doing this, researchers place the phenomena under study in its cultural and social context (Myer, 1997). The main advantage of ethnography is the first-hand collection of data. However, it is challenging for the extensive time needed to collect data and the integration required may compromise the researcher's objectivity in the study (Bryman and Bell, 2015; Rosen, 1991). Studies conducted in this way are written in a literary, storytelling approach which is not scientifically inclined (Myers, 2009). Ethnography will not be used in the present study because the phenomenon under study is not restricted to a socio-cultural site or a distinctive social group. Furthermore, because "a good ethnography requires prolonged stay at the research site" (Wolcott, 2008) to observe and interact with the research participants, the constraints of time and finances to enable this stay makes ethnography inappropriate for this study.

5.4.2 Case Study

A case study is defined as:

> *An empirical inquiry that investigates a contemporary phenomenon within its real-life context; when the boundaries between phenomena and the context are not clearly evident, and in which multiple sources of evidence are used. It is particularly valuable in answering who, why and how questions (Yin 1994, p.23).*

Although a case study method can be quantitative or qualitative (Seawright and Gerring, 2008), the qualitative strand is discussed here. The qualitative case study involves in-depth exploration of a bounded system known as a case (Yin, 2014). The case is usually bound by time and space or other unique characteristics (Seawright and Gerring, 2008; Yin, 2014). Several sources of data such as interviews, audio-visual materials, documents, observation, and reports rich in context may be used to explore the case (Creswell, 1998). Although purposeful sampling may be used to show different perspectives in a case study, a case is usually selected because it is unique and requires in depth investigation.

A case study can be conducted either as a single or multiple case studies. The single case focuses on a unique context of investigation in the research (Denscombe 2003) and looks in depth (Creswell 2007; Oates 2006), aiming to generalise outcomes to a larger population (Yin, 2014). Conversely, in the multiple case studies, the researcher focuses on several cases, usually not exceeding four or five cases for investigation (Creswell and Poth, 2018). Case study research is suitable for both theory building and theory testing because case studies produce rich descriptions as they dig into the experiences of research subjects (Oates 2006). Although case studies produce rich descriptions, it is weak in generalising to scale (Creswell 2007; Oates 2006). In addition, getting access to case sites could be challenging (Recker, 2013).

Although case study seems to fit the aims of the current research as it could enable the gathering of in-depth knowledge about the phenomenon investigated, it will not be used because the number of respondents to be interviewed exceeds the

recommended number of multiple cases. Moreover, the case study is criticised for lack of rigour and reliability (Denscombe 2003; Oates 2006).

5.4.3 Action Research

Most action research studies are interpretive, but they can also be positivist or conducted through critical research paradigm (Avison et al., 2017). Avison et al. (2017) argue that action research is a practical problem-solving method aimed at expanding scientific knowledge and the competencies of research participants. Typically, participants are engaged through real life collaboration with the researcher. In this process, feedback is immediate and cyclical, aiming to increase the understanding of a social situation and the associated change processes. Action research explores real life situations and thus challenges systemic limitations involving researchers and research participants (Myers, 2009). This type of action research is referred to as participatory action research that unifies theory and practice (Avison et al., 2017).

Another variant of action research, though less popular is the action science. This variation seeks to understand participants' behaviours as a basis for developing theories using single and double loop learning process (Atkinson, 1994; Avison et al., 2017). However, what differentiates both forms of action research from other forms of social research is the real-life context it engages to stimulate participatory change (Recker, 2013). This suggests that researchers' involvement in the organisation or community researched should create a shared perspective of the problem and the change anticipated through the process.

Although action research can gain in-depth knowledge about a problem through the researcher and participants' collaboration (Bryman and Bell, 2015), the challenge of submerging into the life of each participant (the smartphone users) due to the amount of time doing this will require, makes this method unfit. Moreover, action research requires researchers to conduct their study within the settings where the problem occurs or where the change is targeted (Recker, 2013). There are no confined communities or settings unique to smartphone users, therefore, this method is unsuitable for the aim of this research.

5.4.4 Grounded Theory

Grounded theory (GT) method requires the researcher's close contact with research participants. This enables interactions and interpretations to occur regarding the phenomenon studied (Goulding, 2002). GT is attractive to IS researchers because through it researchers can understand how individuals think and act in their organisational and social contexts (Orlikowski and Baroudi, 1991; Urquhart et al., 2009). This in turn can produce deep insight into information system phenomena (Klein and Myers, 1999). GT is a qualitative research method aimed at developing theory that is grounded in data through systematic gathering and analysis. According to Charmaz (2003) and Hutchison et al. (2010) GT begins with inductive strategies for collecting and analysing qualitative data. For example, iterative sampling and analysis process. This process is a major difference between grounded theory and other qualitative research methods. Such GT's specific approach to theory development recommends an interchanging process of collecting and analysing data (Creswell, 2003, 1998). This process continues until data is saturated when no new concept emerges from the data. From this process, GT can capture and interpret complex social phenomenon (Charmaz 2003) as they are constructed (Charmaz 2003; Glaser and Strauss 1967; Goulding 1998). Therefore, GT is considered appropriate for this study because privacy decision-making and the various influences on the decision process are complex (Acquisti and Grossklags, 2005; Beldad et al., 2011). More justification for the choice of GT is discussed in the next subsection.

GT has been criticised for lack of rigour resulting from skewed interview techniques that can introduce researcher's bias (Timonen et al., 2018). In this research, the interviews questions were structured objectively to avoid leading questions and researcher bias (Turner, 2010). For example, this researcher asked the respondents "do you have privacy concern when you use your smartphone?" as against leading the respondents by asking, "tell me the privacy concerns you have when you use your smartphone". Additionally, transcribed texts were checked to ensure content accuracy before beginning the analysis. These actions were to minimise the risks of bias. Moreover, the conclusions drawn are grounded in actual data that follows the systematic and rigorous process to discover the concepts that informed emerged

categories. This systematic process is iterative (Alammar et al., 2019; Corbin and Strauss, 1990) and follows the Straussian strand of GT. Table 5.2 summarises the research methods discussed.

Table 5.2 summary of the research methods considered

Dimension	Grounded Theory	Ethnography	Case Study	Action Research
Focus	Field data leads to theory development	Cultural groups are described and interpreted	Single or multiple cases are deeply studied	Empower participants to change status quo
Discipline origin	Sociology	Cultural anthropology sociology	Sociology and political science	Political science, sociology
Data collection	Interviews continues until the data is saturated towards theory	Interviews and observation with additional artefacts and staying long in the field (e.g., 6 months to a year)	Several sources- interviews, observation, physical artefacts	Ethnographic engagement, interviews
Data analysis	Through open, axial and selective coding process	Analyses, describes and interprets	Describes by identifying themes and/or making assertions	Themes Assertions
Narrative form	Theoretical postulation or model	Culture of a group or an individual is described	Case or cases are described or explained	Iterative and cyclical

5.4.4.1 The Rationale of adopting grounded theory for this research

The choice of a research method should be guided by the aims and nature of the research and the research questions (Bryman and Bell, 2015b; Crowther and Lancaster, 2008). As mentioned in chapter one, this research aims to propose a middle range theory grounded in data regarding smartphone users' perception of information sensitivity. Since GT enables researchers to explore and unearth hidden perceptions, it is considered suitable for the research (Alammar et al., 2019; Corbin and Strauss, 1990). Additionally, GT is adopted for the following reasons.

First, the current research adopts the interpretive paradigm and for that reason, using GT is possible. The relativist ontology and the epistemology underpinning GT allows the researcher to accept the knowledge that is socially constructed and interpreted by both researcher and participants (Corbin and Strauss, 1990; Dudovskiy, 2016).

Second, GT is an important method for studying complex social phenomenon such as privacy decisions across different categories of people as undertaken by this research (Corley, 2015). Moreover, by adopting GT, a researcher can identify unique concepts and incidences that sheds light on the differences between categories of people (Glaser and Strauss 1967). The current research seeks to explain the differences in perceived information sensitivity by categories of smartphone users. In addition, Strauss (1998) recommends coding data by "microanalysis" that involves detailed and painstaking "word-by-word", line by line analysis to code the meanings found in the words or "groups of words" (Strauss 1998, p. 68). The usefulness of "microanalysis" is the ability to unearth hidden phenomenon as the data is revisited many times, looking and re-looking for emerging codes. In doing this, other issues may emerge, resulting in further coding and subsequent interviews (Corbin and Strauss, 1990; Corley, 2015). Therefore, GT allows nuances between categories of users to be revealed. This is one way that GT differs from other research methods through the systematic and inductive processes for collecting and analysing data to build theories that explains data (Belgrave and Seide, 2019). From this rigorous and systematic approach, GT sheds light on areas that are relatively complex (Corley, 2015; Urquhart et al., 2009). As discussed in section 5.7, the Straussian strand of GT will be used to achieve the aims of this study. The choice of GT as the research method requires the appropriate data collection method. The choice of data collection method depends on the chosen research method (Pinsonneault and Kraemer 1993). Therefore, the next section discusses the appropriate methods that are compatible with GT.

5.5 Data Collection Methods

Since the current research adopts the grounded theory as the research method, the sources of data that are compatible with GT and the research questions are evaluated. Research questions influences the choice of data collection methods

(Fry et al., 2017). However, no single method of collecting data has complete advantage over others. Therefore, the choice of any data gathering method depends on the aim of the study (Yin, 2014). According to Corbin and Strauss (1990) the sources of data most used with GT are: observation, interviews and document analysis.

5.5.1 Observation

Observation is the method of watching by paying attention in order to capture the activities of interest to the researcher (Fry et al., 2017; Oates, 2006). Furthermore Fry et al. (2017), argues that observation as a data collection method is the systematic collection of data about different settings and groups to understand the phenomena within its context. Since watching is involved, the researcher must be a keen looker without interrupting the process of observation by asking questions (Fry et al., 2017).

Although Jamshed (2014) suggests that people might reveal their experience better by their actions rather than in speech, looking alone is unlikely to reveal deep seated perceptions. Therefore, Fry et al. (2017) argues that observation is better suited for collecting data on processes and not on why people respond to situations. Observation method is used to gather quantitative and qualitative data through the direct and participant observation techniques (Jamshed, 2014). In the direct observation technique, the researcher is passive and neutral, thus, not active in the phenomenon under study. However, the researcher can participate in the phenomenon through the active participant observation process (Recker, 2013). Participant observation can be conducted by smelling, touching and hearing the participants (Oates, 2006), thus making observation a commonly used technique in clinical studies (Fry et al., 2017). However, observation as a data collection method is time consuming, it requires very broad coverage to be effective and is superficial (Fry et al., 2017; Recker, 2013). Therefore, this method is not going to be adopted as the source of data in the current research. Additionally, this method is not consistent with the aims of this study. To understand the perceptions of smartphone users regarding specific critical factors will require individuals telling their stories because perceptions cannot be

accurately observed (Assemi et al., 2018; Xu et al., 2011a). Therefore, exploring users' experiences and views will require more than mere observation method.

5.5.2 Documents

Documents are available or existing data on paper and computer-mediated text, including extra-text formats such as photographs, images, diagrams and graphs (Rapley and Rees, 2018). Therefore, they are static containers of knowledge. Although documents may be updated, they are unable to capture the quickly changing dynamics surrounding individuals' decision process (Ahmed et al., 2018; Rapley and Rees, 2018) such as the complex privacy decision-making process. Since collecting documents from libraries and websites for analytical work is quite simple and cheap, some researchers forgo empirical work to use it (Oates, 2006). However, the credibility of a document in terms of source and content may limit its usage. Using an unreliable document can result in inaccurate interpretation of the phenomenon under study (Oates 2006).

Although document collection could be used as primary data in GT (Strauss and Corbin, 1998), concerning the aim of this research, document collection is not chosen as the primary source of data. This is because the phenomenon studied requires in-depth exploration to unearth contextual cues and hidden nuances across different categories of users in ways that static documents may not accurately allow (Rapley and Rees, 2018; Wünderlich, 2010)

5.5.3 Interview

According to Orlikowski and Baroudi (1991), the qualitative interview method is the primary tool used by grounded theorist to collect data for studying empirical reality. Researchers use interviews to discover non-linear concepts grounded in the data to build theory (Wünderlich, 2010). As GT is not a linear process, the iterative and comparative process requires an interactive and interrogative method such as the qualitative interview (Chun Tie et al., 2019; Wünderlich, 2010).

Qualitative interviews are loosely structured to allow the interviewer and the respondent explore issues and unearth new insights. These insights unfold complex processes and provide descriptive data about people's behaviour, attitudes and perceptions (Wünderlich, 2010). Most qualitative research interviews are the semi-

structured type (Mason, 2002). In contrast to the unstructured version, the semi-structured interview allows the researcher to ask standard set of questions. Although the questions are standardised, respondents can answer in different levels of depth (DiCicco-Bloom and Crabtree, 2006; Wünderlich, 2010) and the researcher can change the order of questions based on the flow of conversation (Denscombe 2003). Furthermore, semi-structured interviews allow questions to be tailored towards gathering responses that are relevant to the phenomenon studied (Denscombe, 2003). Such as the questions tailored to elicit the perceived information sensitivity of respondents regarding the influences of location tracking, economic status and app permission requests. This is because the researcher seeks to explore meanings and perceptions about those factors. Therefore, the semi-structured interview is selected for the current research.

Qualitative interviews generally allow the respondents to use words drawn from their own concepts and experiences to provide rich perspectives. The rich diversity of perspectives that interview produces make data gathered in an interview more reliable than data gathered by a list of self-completed questionnaires or obtained from static documents (Chun Tie et al., 2019; Orlikowski and Baroudi, 1991). Since interviews can reveal diverse views on the phenomenon investigated, it will enable the collection of different perceptions of smartphone users concerning personal information disclosure.

Another type of qualitative interview is the focus group (Owen, 2001). Although the focus group can be efficient, it is problematic because one or a few members of the group can dominate the discussion. Issues such as gender bias and technical expertise can influence domination (Denscombe 2003). Additionally, a bandwagon effect could occur in a focus group (Owen, 2001). This is when some members merely concur with a predominant view without expressing personal opinions because of the public nature of the process (Chirban, 1996). This problem makes it difficult for the researcher to discover the rich and diverse perspectives required (Denscombe, 2003; Owen, 2001) To avoid this, the current researcher prefers to conduct the one-to-one interviews to gather diverse perspectives on privacy issues from smartphone users. Moreover, in a one-to-one situation, it is

possible for an interviewer to know if participants are suitable for answering the questions. Participants are freer to discuss the issues in detail and the interviewer can clarify points (Jamshed, 2014; Orlikowski and Baroudi, 1991). Although the one-on-one interview provides depth, it has been criticised for lack of diversity compared to the focus group that enable interviewers to get a wider range of experiences (Owen, 2001). To address this, a diverse range of respondents from the academia and industry (marketers, advertisers and app developers) were purposively selected for the research.

The researchers view regarding how social reality is constructed affects the choice of a suitable methodology, including the tools used to collect data. The research aims and the nature of the research questions contributes significantly to this decision. In this research, the qualitative one-to-one and semi-structured interview is considered the most appropriate method for collecting empirical data. This choice is influenced by using the interpretivist paradigm and grounded theory in the study. The Research of this nature requires rich data that will provide deep understanding of the socially constructed phenomenon investigated. The following sub-section present how the interviews are conducted in the study.

5.5.3.1 The interview questions and respondents

The questions prepared for the respondents are shown in Tables 5.3, 5.4 and 5.5 below. However, the semi-structured nature of the interviews gives the researcher the flexibility of not always asking the questions verbatim or following the numerical order presented in the table. The current researcher only rephrased the wordings of the second question once with one respondent when clarification was sought. On that occasion, the question was rephrased as: “have you ever had an experience of privacy breach through your smartphone?”. Therefore, the extent of flexibility applied during the interviews was very minor.

Table 5.3: The semi-structured interview questions for the first round of interviews

First Round of Interviews			
S/N	**Questions for smartphone users**	**Purpose of question**	**Alignment with Literature/theory**
1	Do you have privacy concerns when you use your smartphone online? (then follow up questions) If yes, what are they? If no, why?	To explore users understanding of privacy risks and the link to perception of information sensitivity	Users understanding of privacy risk may be bounded (Acquisti and Grossklags, 2005; Simon, 1982)
2.	What has been your experience with improper invasion of privacy through your smartphone?	To explore the link between previous privacy experience and perception of information sensitivity.	Privacy breach affects privacy mitigation (Armando et al., 2015; Park et al., 2019)
3	In general, would it be risky to give personal information through your smartphone? If yes, what might be the consequences? If no, why?	To investigate the link between risks perception and users' privacy concern category	Users differ and may perceive privacy differently (Dhawan et al., 2014; Knijnenburg, 2017)
4	What motivates you to disclose your personal information via your smartphone? (Researcher to ask question B. if interviewee is totally blank on question A). For example, is it monetary or time saving benefit?	To understand varying influences of benefits of using the smartphone	Immediate gratification influences privacy trade off (Acquisti, 2004a; Rochelandet and Acquisti, 2011)
5	Through apps permission request, most apps ask for specific access to users' information required for functionality. How willing are to allow access to your personal information such a location? And why?	To explore the influence of location tracking on disclosure	Location tracking yields implicit information (Cabalquinto and Hutchins, 2020; Kokkoris and Kamleitner, 2020)

6	Through apps permission request (APR), most apps ask for specific access to users' information required for functionality. Is there anything you want to tell me about apps permission request? For example, does it affect you in any way?	To explore the effect of app permission request	App access users' information beyond authorisation (Boateng et al., 2019; Degirmenci, 2020)
7	Does apps permission request affect how you feel in terms of information sensitivity? If yes or no how does it make you feel?	To explore users understanding of the risks posed by app permission	To help tailor RALC publicity rule (H. Tavani, 2007; Tavani, 2008)

Table 5.4: The semi-structured interview questions for the second round of interviews

Second Round of Interviews			
	Questions for smartphone users	**Purpose of question**	**Alignment with Literature/theory**
1	What issues are important to you about your information privacy online? Why are they important?	To explore other factors and the situations that influence information sensitivity	Information sensitivity is situation specific (Bansal et al., 2016, 2010a; Mothersbaugh et al., 2012)
2	What kinds of information in your smartphone or that may be accessed through it are particularly sensitive to you (for example, information about your activities, movements, photos/videos or contacts etc.)?	To explore how users perceive various types of information	Information sensitivities vary with information type (Degirmenci, 2020; Furini et al., 2019)

Table 5.5: The semi-structured interview questions for the third round of interviews

Third Round of Interviews			
	Questions for smartphone users	**Purpose of question**	**Alignment with Literature/theory**
1	How do you relate your income status to your concern for personal information that may be accessed through your smartphone?	To further explore the link between user sensitivity and economic status	Economic status influences decision making (Carrascal et al., 2013; Sheehy-Skeffington and Rea, 2017)
2	What kinds of information in your smartphone or that may be accessed through it are particularly sensitive to you?	To confirm concepts emerging in the data regarding types of sensitive data	Theoretical sampling explores emerging concepts to data saturation (Alammar et al., 2019; Strauss and Corbin, 1998)

The questions asked during the second and third rounds of interviews are in addition to the prior questions. The interview respondents in this study were selected through a combination of convenience and purposive sampling methods which are nonprobability in nature. Nonprobability sampling does not use random selection methods, rather it is a sample selection method based on the purpose of the study. It is useful for selecting a subset of people because of the relevant information they can provide (Palinkas et al., 2015). In the current research, respondents are selected to understand the differences in perceived information sensitivity regarding the collection of personal information during smartphone use.

According to Palinkas et al. (2015), selecting in-depth interview respondents based on purposive sampling aims to maximise the depth and richness of the data required to address research questions. Thus, purposive sampling is suitable for selecting subject experts. Subjects experts in the context of this research are people with evident knowledge of privacy and the smartphone context because they work in related fields. For example, two mobile app developers, two managers in mobile advertising agencies and three academics in privacy related fields were among the respondents. In general, the respondents were recruited from the staff and PhD

students at De Montfort University Leicester, Birmingham City University and others from outside the universities.

Respondents were purposefully selected to ensure they have basic privacy-related knowledge by ensuring that participants have a university degree. Turow et al. (2009) investigating consumers' understanding of privacy rules in the marketplace found that respondents educational level correlates with basic knowledge of privacy. Similarly, Surma et al. (2012) found that first degree level education exposes students to basic privacy literacy. This suggests that respondents' views are indirectly influenced by basic knowledge of privacy. Tables 5.6 and 5.7 below summarises the sources of data that are used in this research and their identity code. For the rest of this research, respondents will be referred to by their identity code.

Table 5.6: Summary of the sources of data

Characteristics (47 participants)				
Economic Status	**Guardian**	**Pragmatist**	**Unconcerned**	**Income group total**
High income	7	9	6	22
Middle income	6	3	5	14
Low income	5	3	3	11
	18	15	14	

Table 5.7 Characteristics of interviewees and labels

S/N	Participants label for economic status factor	Characteristics	
1	Hi-PG 01 - Hi-PG 07	High income	Privacy guardian
2	Hi-PP 08 – Hi PP 16	High income	Privacy pragmatist

3	Hi -PU 17 – Hi-PU 22	High income	Privacy unconcerned
4	Mi -PG 23 – Mi-PG 28	Middle income	Privacy guardian
5	Mi-PP29 – Mi-PP 31	Middle income	Privacy pragmatist
6	Mi-PU 32 – Mi-PU 36	Middle income	Privacy unconcerned
7	Li- PG 37 – Li-PG 41	Low income	Privacy guardian
8	Li-PP 42 – Li-PP 44	Low income	Privacy pragmatist
9	Li-PU 45 – Li-PU 47	Low income	Privacy unconcerned

5.5.3.2 Interview protocol

To ensure the success of the research process, an interview protocol was developed. Before conducting an interview, the interview fact sheet containing the purpose of the interview is emailed to participants as well as asking for a date and time for the interview. Participants are also required to give formal consent by signing the consent declaration form that clearly states the interviewees' rights regarding their confidentiality and how data will be treated (see Appendix C). Additionally, the researcher will ask participants for permission to record the interviews on an audio digital recorder. A background information sheet is then filled after which the interview will commence.

The pre-interview background information sheet is designed to capture income status and Westin's privacy concern category of the respondent. Respondents' income status determined their assignment to either high, middle, or low economic status group and disposable income indicated respondents' income status (see tables 5.4 and 5.5). According to the UK Office of National Statistics (2017), disposable income is widely used to measure income. This is the money that is available for spending and saving after direct taxes have been paid by

individuals. The UK disposable income measure is used because it matches the research setting. Hence economic status is categorised into 3; high (£25,001.00 and above) middle (£25,00.00 - £12,501.00) and low (£12,500.00 or less). A similar approach was used by Acquisti and Grossklags (2005) when they collected individuals' economic data to understand the multiple factors affecting privacy decision-making. Their study identified the lowest income group in the US as those with disposable income below $15,000 a year. Furthermore, to categorise respondents into the privacy concern categories, Westin's original questions were used to group respondents (Kumaraguru and Cranor, 2005). Respondents' answers to the questions were analysed according to Westin's analytical scheme to group the respondents into one of the three privacy concern categories, that is, privacy guardians, pragmatist and unconcerned (see Appendix C).

The interviews were conducted in three cycles to fill up gaps in the emerging concepts during the analysis process. The first cycle was conducted between 06/2018 and 07/2018, the second cycle from 01/2019 to 02/20109 and the third was between 09/2019 and 10/2019. The interview protocol ensured that participants in this research should be confident that their information will be protected and used as declared by the researcher. This researcher conducted a pilot study to gain experience with the field work and to test whether the research questions were accessible and if the research aim could be achieved.

5.5.3.3 The Pilot study

According to Vogel and Draper-Rodi (2017) pilot studies are designed to test methodologies and to assess the feasibility of initial ideas before launching into a larger study. Pilot studies reduce the chance of abandoning studies at a later stage. Through pilot studies, researchers can refine data collection tools and gain experience with data analysis procedure. Therefore, researchers can produce more credible outcomes due to improved analytical skills (Malmqvist et al., 2019; Vogel and Draper-Rodi, 2017). Additionally, Malmqvist et al (2019) argues that pilot studies are important parts of the research process which are often neglected. Consequently, the current researcher conducted a pilot study to test the initial interview questions among 7 smartphone users in De Montfort university Leicester, UK. The results of the pilot study were used to revise and refine the research

questions (see table 5.8 below). The ethical issues considered in this research are discussed in the next sub-section.

Table 5.8: Examples of revised interview questions after the pilot study.

Initial Question	Revised Version	Reason for the Revision
Do you have privacy concerns when you use your smartphone online?	Do you have privacy concerns when you use your smartphone online? (then follow up questions) If yes, what are they? If no, why?	Responses were a short yes or no. Follow up questions allowed deeper probing
What are the risks in sharing information through the smartphone?	In general, would it be risky to give personal information through your smartphone? If yes, what might be the consequences? If no, why?	The question was personalised as most respondents thought that a nonpersonal view was solicited.
What will motivate you to disclose personal information via your smartphone?	What motivates you to disclose your personal information via your smartphone? For example, is it monetary or time saving benefit? Follow question up is asked if interviewee is totally blank.	Most pilot respondents were unclear about what motivation in this context means.

5.5.3.4 Ethical Issues

The success of the research also depends on how the human subjects who are the sources of data are treated. Participants' privacy is an important issue, therefore, confidentiality and anonymity should be considered in the research (Lindorff, 2010; Page and Nyeboer, 2017). Moreover, De Montfort University's regulations requires a formal ethical approval before the research student engages in data collection activities involving human subjects. Accordingly, the current researcher had received the approval of the human research ethics committee (see Appendix A).

The overriding principle of the 2015 guidelines for good research practice in DMU[40] is that there "must be no harm caused by the research investigation or the dissemination of its results".

Since this research does not pose any type of potential harm to participants, the researcher informed the participants about the purpose and nature of the research. Participants were accordingly asked to sign the consent form (see Appendix B).

Finally, to fulfil the objective of the ethical guidelines, the researcher was honest with the participants regarding every clarification sought. Additionally, participants' privacy was respected when posing the interview questions by not delving into areas they did not want to elaborate on. In doing this, the researcher assured participants of confidentiality and anonymity. Hence participants are represented by anonymised codes in the data analysis.

5.6 The analysis Processes

To achieve the aims of this research as discussed in chapter one, the Interpretive paradigm, the Straussian Grounded Theory, and semi structured interview were used. The semi-structured interview is used to collect empirical data to answer the second and third research questions.

5.6.1 Data Analysis: Grounded Theory

GT is a symbolic interactionism method (Heath and Cowley, 2004) that focuses on the relationships among individuals within a society. Through GT, researchers look at the exchange of meanings and how individuals make sense of their social worlds as they actively shape it (Jensen et al., 2016). Strauss and Glaser introduced the grounded theory method and suggested that a theory can be generated by applying its systematic and qualitative analysis techniques (Charmaz 2006).

---

40 Available at:https://www.dmu.ac.uk/documents/research-documents/ethics-faculty-procedures/ethics-and-governance-general-/dmu-guidelines-good-research-practice.pdf

According to Glaser and Strauss (1967), GT systematically analyse data to achieve the following: (1) enable behaviour to be explained and predicted, (2) to develop theories, (3) allow researchers to understand and gain control of situations, and (4) unearth different perspective on issues. This suggests that the theory that achieves all these aims should fit the following criteria: (1) theoretical categories should represent the data in relevant and understandable ways, (2) the core idea that emerges should explain what happened, (3) the theory should be predictive, (4) able to interpret what is happening, and (5) can be modified every time new data is collected (Corbin and Strauss, 1990; Glaser and Strauss, 2009). When a systematic discovery of theory from the data meets the above criteria, such theory is difficult to refute. The methods of constant comparative analysis and theoretical sampling are key characteristics of GT. They entail generating patterns and concepts from data, which can result in further coding and analysis (Glaser and Strauss 1967). The next sub-section discusses these characteristics.

5.6.1.1 Constant comparison

The constant comparison method generates theory systematically by combining coding and data analyses concurrently (Glaser and Strauss 1967). The method involves theoretical sampling that enables flexibility in generating theory by seeking additional data based on the initial concepts developed in the analysis process. The constant comparison stage is designed for: (l) comparing the coded concepts that are applicable to each concept category, (2) integrating the emerging categories, (3) determining the theory, and (4) writing the theory (Glaser and Strauss, 1967, p. 3). The constant comparison stage allows the analyst to discover critical points in respondents' discourse that remains vague and requiring clarification from respondents. Furthermore, constant comparison "is to stimulate thinking about properties and dimensions and to direct theoretical sampling" (Strauss and Corbin, 1998, p. 78), that can lead to further interviews based on the emerging theory.

5.6.1.2 Theoretical sampling

Theoretical sampling refers to the cumulative process of data collection to generate theory (Corbin and Strauss, 1990; Glaser and Strauss, 2009). In other words, the decisions of what data should be collected is controlled by the emerging theory. Concepts that have proven theoretical relevance to the emerging theory can be

developed and revalidated by new data. The process helps the analyst to determine further collection of data that enables the analyst to discover and fill gaps in the emerging theory (Glaser and Strauss 1967). The technique of theoretical sampling is applied during both the data collection and analysis processes (Glaser and Strauss 1967) and establishes a relationship between emergent concepts and categories through their properties and dimensions leading to theory development (Strauss and Corbin, 1990).

Given the aim of this research, the researcher used interviews as the data collection instrument in order to draw in-depth understanding from the participants, who have first-hand experience of how smartphone use data collection influences perception of information sensitivity. For example, after the first and second rounds of interviews, it was still unclear how and why economic status influenced the concern for personal information that could be collected through the smartphone. Therefore, in the third round of interviews, this researcher purposively looked for participants that belonged to the high, middle and low economic status groups and specific questions about the connection between their economic status and the concern for their personal information that could be collected through the smartphone were asked (see table 5.5). Since theoretical sampling is purpose-specific, it is considered as a form of purposive sampling (Strauss and Corbin,1990). Therefore, theoretical sampling assists the researcher to choose the right people to interview during the data collection process. Finally, theoretical sampling process is designed to stop at the point of saturation when data no longer yield new concepts. This is the point where concepts are getting repeated.

Two kinds of theories, *substantive* and *formal* can be developed from GT analytical techniques. “Substantive theory is developed from a substantive area of sociological inquiry, whereas a formal theory is developed for a formal area of sociological inquiry” (Glaser and Strauss 1967, p.32). A substantive theory focuses the research on one substantive (empirical) area. For example, the smartphone-use data collection and comparing users’ perceptions within that single area. In contrast, a formal theory focuses on more abstract or conceptual area of research by comparing different substantive areas. The currents research develops a substantive theory because the researcher focuses on a substantive area of inquiry, that is, the differences in

perceived information sensitivity due to smartphone use data collection. In addition, this research compares the perceived information sensitivity of users with different privacy attributes. Therefore, the generation of a substantive theory through a comparative analysis within the same area is possible (Glaser and Strauss,1967). However, Glaser and Strauss disagreed on the best way to generate theory from data. This divergence will be discussed in the next sub-section.

5.6.1.3 Glaserian vs. Straussian strands of GT

Although GT has undergone several iterations by other authors since its initial conception, the most visible variation is between the conceptions of the two initiators: Glaser and Strauss (Heath and Cowley 2004). The differences between the two versions are discussed in this sub-section.

The two main strands of grounded theory are the Glaserian and Straussian strands (Locke 1996). According to Locke (1996) there are no significant differences between the Glaserian and Straussian strands in their main analytical procedures, such as constant comparison and theoretical sampling explained earlier. The divergence lies in the relationship between the researcher and the field of investigation. Others have described the differences between the Glaserian and Straussian strands as methodological rather than ontological or epistemological in character (Alammar et al., 2019; Wolfswinkel et al., 2013). The Straussian strand uses different analytic techniques. There are several differences between the two originators. First, while the researcher is expected to have an active role in the research process by becoming immersed in the data at a detailed level to allow coding of concepts in the Straussian strand, such active role is not expected in the Glaserian strand (Alammar et al., 2019).

The second difference lies in the conceptualisation process (Urquhart et al., 2009). In the Straussian strand, conceptual labels representing a phenomenon is given to each observation which is a unique occurrence in the data. Glaser argues that developing every observation into a concept leads to over-conceptualisation and recommends that the researcher should rather compare each incident (occurrence of a social process) with other incidents (Alammar et al., 2019).

The third difference between the two relates to the suggestion by Strauss about using questions such as *when, who, what* and *which*. Glaser argues that doing this imposes preconceived categories into data (Charmaz 2006). Rather, Glaser suggests a few neutral questions like: *What property or category does this incident indicate?", "what is this data a study of?*

Fourth, the role of literature in the research process differs in the two strands. Although there is consensus that the researcher needs background ideas about the field, they disagree on the role literature should play (Heath and Cowley 2004). In the Straussian strand, the researcher requires familiarity with literature relating to the phenomenon under investigation as a basis for professional knowledge (Strauss and Corbin, 1998). Similarly, Alammar *et al.* (2019) and Timonen *et.al.* (2018) argues that literature provides guidance for the novice researcher. Conversely, Glaser (1978) criticised the use of literature because it can bias the analyst when interpreting data. Glaser (1978) argues that previous knowledge can direct the researcher's focus. Thus, to be objective, Glaser (1978) recommends that the researcher should suspend background knowledge about the phenomenon being investigated (Timonen et al., 2018). Therefore, reality should be investigated and analysed without preconceived notion (Glaser 1978). Literature should only be explored after the theory has been developed (Timonen et al., 2018). Table 5.9 summarises the differences between the two strands.

Table 5.9: Summarises the main differences between Glaserian vs. Straussian Approaches

	Glaser & Strauss/ Glaser	**Strauss and Corbin**
Researchers role	The researcher has no active role in the research process.	The researcher plays an active role and immersed in data to guide conceptualisation
Conceptualisation process	Compares incidents rather than developing several concepts.	Develops several concepts based on the occurrence of phenomenon of interest.
Types of questions guiding research	Use of neutral questions to discover relationships	Use of questions such as when, who, what and which to guides

	between incidents, property, and categories.	development of concepts and categories.
Data gathering	Interviews are not guided. It follows preconceptions as interviewees are thought to be the experts who will reveal the important issues. Field notes, historical documents, photos, news articles and others can be used to clarify concepts.	Interviews are unstructured; observation is also used to gather data. The researcher interprets data but can clarify with participants.
Data analysis	Researcher continues to sort memos until main concepts becomes clear. Then the theoretical connections between concepts are documented.	Researcher continues analysis until data is saturated
Use of Literature and theory	The researcher is expected to suspend background knowledge about the phenomenon being investigated	Researcher requires familiarity with extant literature thus uses theory to guide theory development.

To conclude, this researcher chose the Straussian strand of GT to guide the collection and analysis of data for the following reasons. First, this researcher lacked enough previous knowledge about data collection in the context of the smartphone and what critical factors could influence users' privacy decisions. Therefore, the Straussian approach fits such novice researcher, by allowing this research to begin with exploring the literature in contrast to the Glaserian strand where the researcher enters the domain directly through data collection and back to the literature at the end of empirical data analysis.

Second, the ontology and epistemology underpinning the two strands are not different, therefore, this researcher chose the Straussian strand because of the robust methodological and analytical procedures (Heath and Cowley, 2004). The analysis procedures make the Straussian strand more systematic than the Glaserian

approach (Alammar et al., 2019; Urquhart et al., 2009). Accordingly, this researcher actively deploys the following analytic procedures in the research.

5.6.1.4 Straussian GT procedures

The following section discusses the procedures that are applied within the Straussian strand of GT. These are open and axial coding.

1.Open coding:

According to Strauss and Corbin (1990, p.61) open coding is "the process of breaking down, examining, comparing, conceptualising, and categorising data". Coding of data begins with the "*conceptualisation process*". In this process of coding as exemplified in chapter six, concepts are characterised by comparing incidents (the empirical data that indicates the occurrence of a new concept or category), sentences and paragraphs in the data. The researcher then labels or names the phenomenon accurately (Corbin and Strauss 1990; Strauss and Corbin 1990).

In labelling concepts, questions such as: what is this? What does it represent? guides the coding activity. Therefore, analysis in grounded theory is driven by "making of comparisons" and "asking questions". Hence, the literature refers to grounded theory as the "the constant comparative method of analysis" (Glaser and Strauss 1967). In addition, *memo* writing, where the researcher records thoughts, interpretations, questions, and directions during the analysis which could lead to further data collection is an important aspect (Strauss and Corbin 1998).

The next stage is "*categorising*". In this stage the concepts that emerged are compared with each other. Concepts that relate to the same phenomenon are grouped together forming categories (Corbin and Strauss 1990; Strauss and Corbin 1990). This process is also guided by asking question such as: what are these concepts about? Thus, making it easier to categorise. Furthermore, each category is given a "name" that differentiates it from other categories. The researcher could form the name, or a name could come from the literature or theory, or from the respondents which is referred to as "in vivo" naming (names drawn verbatim from respondents). Where the name comes from is not as important as the activity of naming the categories (Strauss and Corbin 1990, 1998). Categorising of concepts

reduces the number of units (Strauss and Corbin 1998). In addition, sub-categories which relates to the main category are developed together. The linking of categories with sub-categories is an important aspect of open coding. This is applied by identifying similarities in properties and dimensions. Properties are the attributes or characteristics that pertains to a category. Dimensions relate to the locations of properties along a continuum (Strauss and Corbin 1990). In addition, the researcher uses questions such as: *how*, *where*, and *when* to discover the properties of each category that might also have sub-properties.

2.Axial coding:

Axial coding is defined as “a set of procedures for putting data back together in new ways after open coding” (Corbin and Strauss, 1990, p. 96) To achieve this, the researcher makes connections between categories and their sub-categories by applying the paradigm model (a coding guide for making meaningful extraction from data) that allows the analyst to think systematically about the data. The paradigm model guides the researcher on a consistent path of inquiry from the causal conditions to the consequences of the phenomenon (Corbin and Strauss 1990; Strauss and Corbin 1990). Figure 5.1 illustrates the path of inquiry, leading from one variable to another.

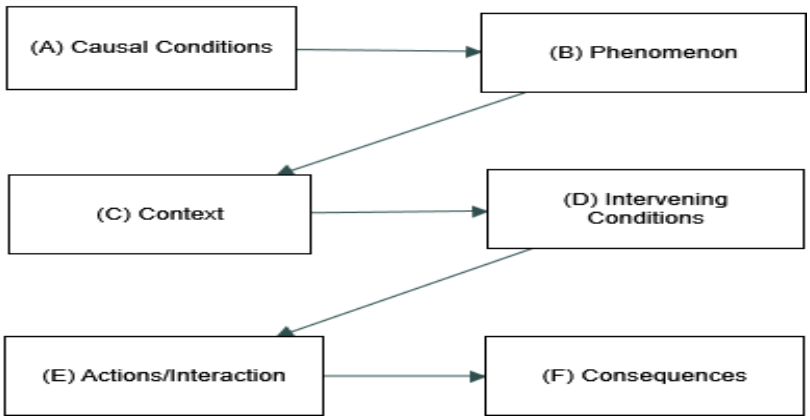

Figure 5.1: Paradigm Model in Axial Coding.

- **Causal conditions**: experience and happenings that bring about the occurrence of a phenomenon.

- **Phenomenon**: the happenings, situation, or experience or the set of actions or interactions being managed.
- **Context**: the conditions under which the happenings/interactional strategies are taken.
- **Intervening conditions**: the conditions impacting the happenings and interaction strategies influencing the phenomenon.
- **Action/Interaction**: strategies for managing or responding to the phenomenon under a specific set of conditions.
- **Consequences**: the resultant effects of actions and interactions

Axial coding develops data towards the last stage of coding, which is the selective coding. According to Corbin and Strauss (1990, p.116) selective coding is "the process of selecting the core category by systematically relating it to other categories, validating those relationships, and filling in categories that need further refinement and development".

For example, this researcher identifies eleven unique concepts and two categories in the open coding stage among high economic status respondents. During the axial coding stage and by applying the paradigm model, one category emerged. This was made possible by re-examining the two initial categories from which a more abstract one that captures the whole story emerged (Strauss and Corbin 1990). The emerged category is the core category, which is the central phenomenon. This technique is applied to find the results presented in Chapter six.

Finally, implementing GT requires proficiency in the coding procedures (Strauss and Corbin 1998). Figure 5.2 below shows the procedures that the Straussian strand of GT recommends. Following this recommendation, the validation process which is the last stage of GT is discussed in terms of how the current research applies the process.

5.7 The Validation Process in Grounded Theory

The validation process of GT research points to the trustworthiness of the research process (Strauss and Corbin 1990). Since GT approaches differs, the resultant validation process of GT depends on the strand of GT a researcher adopts (Charmaz 2006). While the Straussian approach adopted in the current research has inherent

validation process through its analytic techniques (See section 5.61.), other researchers (Sikolia et al., 2013) argue that GT validation process should follow a different process. However, the Straussian GT validation process applied in the current research corresponds to the process recommended by Sikolia et al. (2013), According to Sikolia et al. (2013), GT researcher could ascertain the credibility, transferability, dependability, and confirmability of the research. Credibility is the extent to which the data collected reflects the various aspects of the phenomenon. Similarly, credibility is ensured in the current research through the process of constant comparison (Strauss and Corbin 1990). In this process, the concepts developed from the empirical data are continuously compared with the emerging phenomenon and where gaps exist, other rounds of interviews are conducted until the gaps are filled. This explains why the current research conducted 3 iterative rounds of interviews (See section 5.5.3.1). The process of iterative interview ensures that empirical data accurately reflects the different realities of the phenomenon because it allows this researcher to obtain clarification from respondents.

In continuing the validation process, the current researcher provided clear descriptions of research participants in order to ensure transferability (See section 6.1.1). According to Sikolia et al. (2013), transferability is how well a research finding can fit into another context.

Dependability is another validation process applied in the current research. In doing this, this researcher as a PhD student relied on the expertise of one of his supervisors who is a qualitative researcher to validate and guide the research. Thus, ensuring that the GT procedures are correctly followed.

Finally, confirmability in the validation process aims to make it possible for another researcher to confirm the research findings when presented with the same data and analytical technique. To enable confirmability, this researcher presented the analysed verbatims in Chapter 6 and rich descriptions of participants, including the coding process and how the theoretical propositions were developed (See sections 6.1.1, 6.1.2 and 6.1.3). In addition, other theories have been used in Chapter 7 (see section 7.6) to validate the research findings as recommended by Strauss (1998).

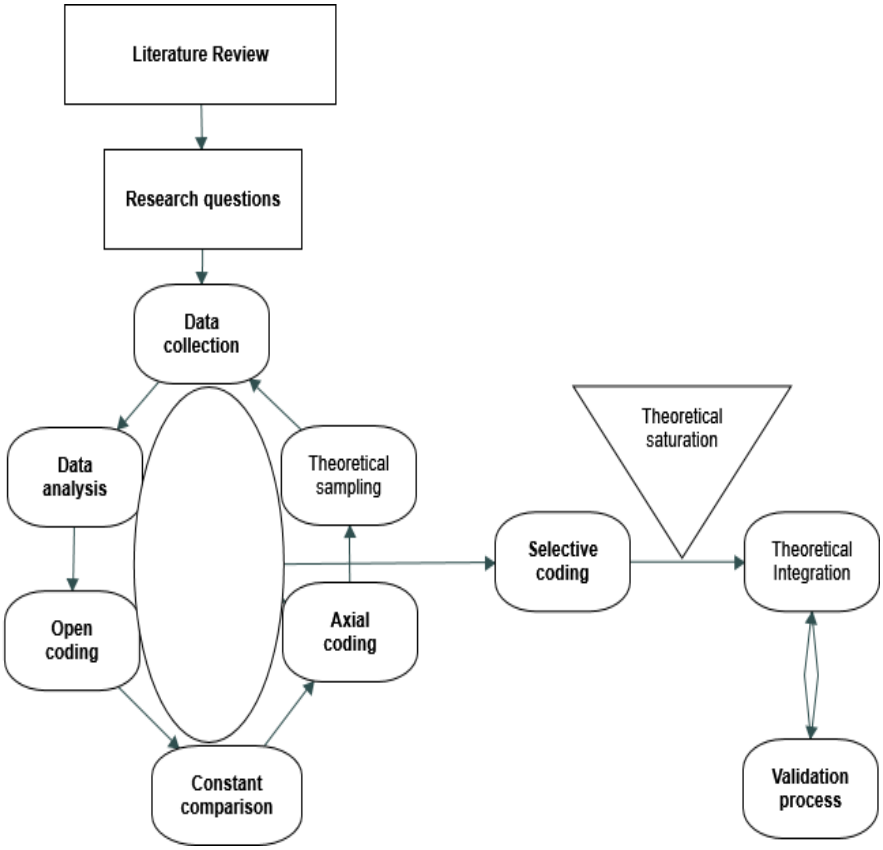

Figure 5.2: The Grounded Theory process

Figure 5.2 illustrates the paths that researchers adopting the Straussian GT follow. First, the research area to be investigated is determined and followed by literature review to enhance theoretical sensitivity. Second, the research questions that directs the investigation are constructed. Third, the field study is undertaken to gather empirical data for the analytical process, and fourth the theory is integrated to explain the phenomenon investigated based on the data. These techniques have been discussed in section 5.6. One way that GT allows the collection of rich empirical data is through the qualitative interview that is adopted in this research (Turner, 2010). As previously mentioned, interviews provide in-depth information about the experiences and perceptions of respondents on the phenomenon studied (Dempsey et al., 2016; Turner, 2010). The researcher can use computer software to support analysis of interview data. However, the software cannot

replace the analytical skill of the researcher. The next section discusses the importance of computer software in assisting data analysis.

5.8 Computer-Assisted Qualitative Data Analysis Software (CAQDAS)

Majority of qualitative researchers are faced with analysing large volume of data. Therefore, Braun and Clarke (2013) and Woods et al. (2016) recommends the use of Computer Assisted Qualitative Software (CAQDAS) in data analysis to save time.

Woods et al. (2016*)* identified three well-known CAQDAS and their distinguishing features. These features partly influenced the choice of CAQDAS for this research.

- NVivo- Interface like Microsoft Outlook; advanced querying functions; and powerful source data and coding organisation.
- MAXQDA- Interface is clean and intuitive; good use of colour for separating project elements; and integrates qualitative analysis well with quantitative analysis features.
- ATLAS ti- Advanced multimedia support; native PDF support with Google earth embedded in it.

These CAQDAS facilitates data analysis process through their unique features by increasing efficiency and enabling transparency of the process (Woods et al., 2016). Furthermore, CAQDAS keep track of data and ongoing analysis as well as supporting the accuracy of the process. The choice of CAQDAS amongst others, depends on the kind of data a researcher is dealing with. For example, MAXQDA will be a good choice for mixed-method research due to its ability to handle both qualitative and quantitative data.

Another choice consideration is the cost of purchasing the software. Datatype and cost influenced the choice of NVivo12 as a data analysis tool for this research. This is because the researcher is dealing with text data which fits into NVivo. Also, the research institution, De Montfort University (DMU) has a site licence for the software that allows the researcher to use it at no cost. Moreover, NVivo has “advanced querying functions and powerful source data and coding organisation” (Woods et al., 2016). In other words, NVivo was chosen as a data analysis support

tool due to its ability to deal with large volume of data, allowing the researcher to channel time saved to the interpretation and creative dimensions of the work (Woods et al., 2016).

5.8 Conclusion

This chapter has discussed three philosophical paradigms commonly used by information systems researchers. These are, positivism, interpretivism and critical research. Various research methodologies and the associated data collection tools have been clarified in this chapter. The aim of this research which is to understand the differences in perceived information sensitivity among smartphone users requires the researcher to employ the interpretivist paradigm in the study. This is because perception is socially constructed and can only be understood through the lens of the paradigm that sees reality as a social construct (Dudovskiy, 2016; Oates, 2006). Therefore, the grounded theory method that can gather this type of subjective data is employed in the study. Regarding data collection tools, the semi-structured interviews are used to collect data. Additionally, the chapter discussed the suitability of the Straussian strand of GT as the appropriate option for the research and finally, the chapter considered ethical issues bothering on the research to ensure the privacy and confidentiality of research participants. The next chapter demonstrates how the methodology described is implemented to obtain the results and findings of the research.

Chapter Six

6. Results and Findings

6.1 Introduction

This chapter presents the results and findings from analysis of the interview data collected from smartphone users in the UK, using a grounded theory approach. The analysis discusses how different categories of users perceive information based on the influences of the three critical factors, which are: Users' Economic Status, Location Tracking and Apps Permission Requests. This analysis also incorporates the varied responses from the privacy guardian (PG), privacy pragmatist (PP) and the privacy unconcerned (PU) categories. There are a number of similarities across categories, but perception of information sensitivity is significantly moderated by users' economic status. Perception of information sensitivity decreases with users' economic status except among the PGs.

The chapter features five main sections, the first section 6.1 provides the introduction which includes participant profiles, data analysis process and building of the theoretical proposition. The second section 6.2 presents the results on economic status from income groups in the three privacy categories. The third section 6.3 discusses the concern surrounding location tracking from the three privacy concern categories. The fourth section 6.4 focuses on the privacy concern caused by app permission request among the privacy categories. Sections 6.2, 6.3 and 6.4 are further structured by themes from the theoretical framework. Concepts that are influenced by the same theme are grouped together for further discussion in chapter seven. The final section 6.5 provides the conclusion of the chapter.

6.1.1 Participants Description

The UK residents interviewed were 47 participants comprising PhD students (20), academics (9), app developers (2), digital marketing practitioners (6) and self-employed individuals (10). The participants included 16 female and 31 males. Majority of them are young and older Millennials in the 25-39 age bracket and a few

Gen X (45-54 age bracket), with only one Boomer (55 +). Participants came from diverse ethnic backgrounds. Their nationalities include 7 Africans, 32 British, 4 Arabs and 4 Polish. These participants reflect the ethnic diversity of the UK population and majority have not explicitly suffered privacy breach before except 3 respondents. They all have at least a university degree. Additionally, participants were chosen if they satisfy the following conditions:

- Use a smartphone
- Earn income
- Willing and able to participate

Explicit privacy knowledge was not a factor in choosing participants, instead educational qualification replaced privacy knowledge. Additionally, Westin's privacy concern classification was used to categorise participants into privacy guardians, privacy pragmatist and privacy unconcerned and salary range was used to group participants into economic status - high, middle, and low income. In qualitative research, it is good practice to provide rich background information about participants in order to enable readers determine how to generalise the research findings (Creswell, 2003; Orlikowski and Baroudi, 1991). Therefore, the background questions prepared for participants are presented before the analysis (see table 6.1 below).

Table 6.1:Background questions prepared for interview participants

Questions	**Desired Information**
Age Range (25-44) ___ (45-54) ___ (50+)____ Ethnicity _____ Gender ❑ Male ❑ Female	To determine demography
Experience with online privacy violations? • I have experienced privacy violation before • Someone close to me has experienced privacy violation before • I have not experienced privacy violation before Others, please specify _____	To determine experience of data breach
Is your mobile phone a smartphone? Yes/No	To determine they have a smartphone
For the purpose of this study, economic status has been grouped into disposable-income groups. Which group will you say you belong to? ❑ Upper (Above £25,001.00) ❑ Middle (£25,00.00- £12,501.00) ❑ Low (£12,500.00 or less) ❑ Don't earn income	. To determine their economic status
What is the last grade in school you completed? ❑ "Not a High School grad" ❑ "High School grad" ❑ "College (Trade or Business)" ❑ "University Grad and beyond"	To determine literacy level

6.1.2 The Coding Process

The interview attempts to identify the level of privacy concern that underpin participants' desire to protect economic status, location information and concerns arising from app permission requests. Therefore, concerns expressed or inferred by respondents were coded and labelled as concepts. In line with Interpretive studies, the meanings that participants assign to concepts determined which theoretical theme is relevant to each section (Orlikowski and Baroudi, 1991). Interpretivist studies are not premised on a fixed relationship between theory and data like positivist studies. This explains why the theoretical themes will not be applied uniformly across the sections. In guiding the analysis, the theoretical themes help "to understand the intersubjective meanings embedded in social life . . . [in order] to explain why people act the way they do" (Gibbons, 1987, p. 3). Figure 6.1 illustrates the framing of the analysis by showing that privacy concern reveals information sensitivity which in turn influences the nature of privacy mitigation (G. Bansal et al., 2016; H. J. Smith et al., 2011; Smith et al., 1996).

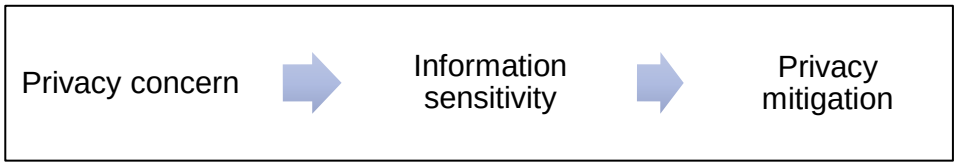

Figure 6.1. Framing of the inquiry and relationship between concepts

6.1.3 Building of the Theoretical Proposition

The research was conducted by following the guidelines of the Straussian strand of grounded theory as described in chapter five specifically subsection 5.7.1. Following the theoretical sampling method, two more interviews were conducted after the first to gradually saturate the data. Figure 6.2 exemplifies the iterative process of GT and how successive interviews produced concepts from high income participants. It illustrates data saturation by showing how concepts emerging from the successive interviews were reoccurring. The same process was followed for all the other factors. Gaps in the data were filled by successive interviews. This process allowed the emerging propositions to be verified retrospectively with participants which serve to assess the robustness.

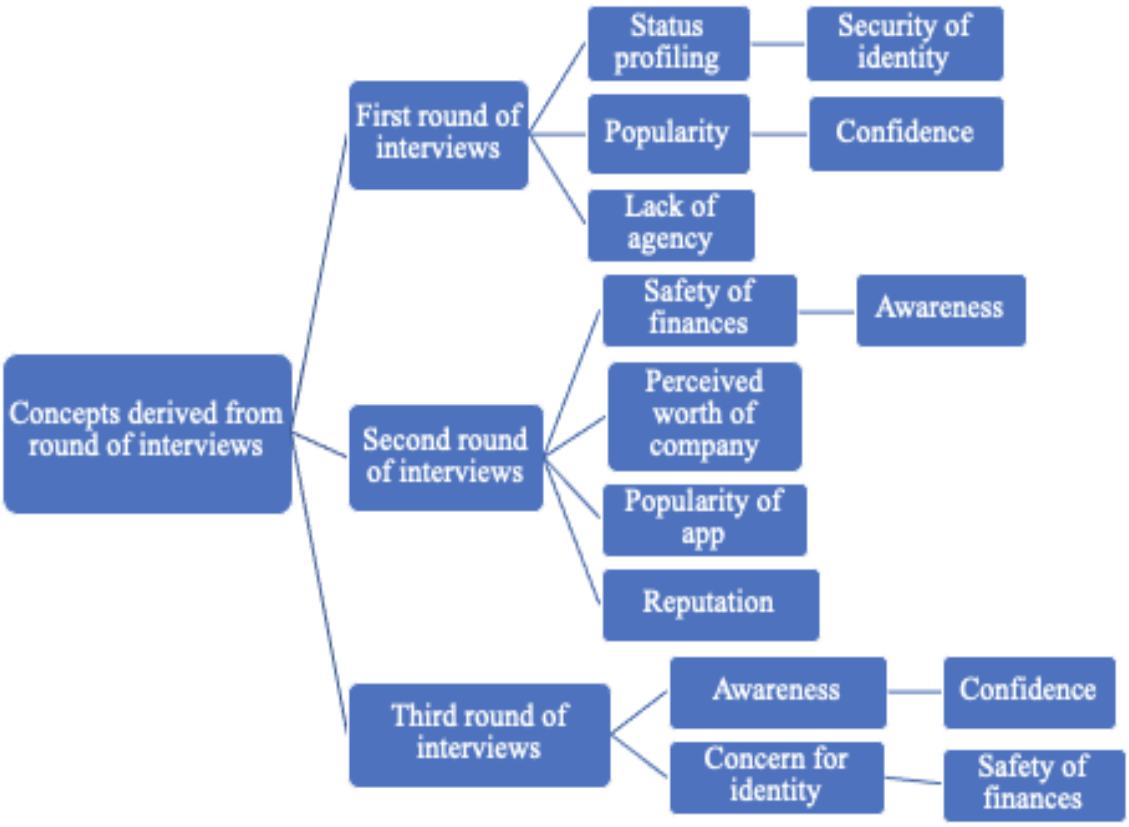

Figure 6.2: Illustrates the iterative process of GT leading to data saturation

6.2 The Influence of Economic Status from the High-Income Group

This section applies the overall coding process of the research, particularly it investigates the influence of high economic status on users' sensitivity to information. The expressed and inferred concerns relating to the protection of economic status and financial information are the types of concepts coded in this section. Two categories have emerged. They are concern for identity and concern for safety of finances. The subcategories are the different dimensions across the distinct income groups. The distinct influences of economic status are revealed by examining the dimensional differences in the concepts across the 3 privacy categories (privacy guardians, privacy pragmatist and privacy unconcerned). For example, concern for

safety of finances is a concern to all the privacy concern categories. However, differences in high or low respondents perceive sensitive information across the 3 privacy concern categories are compared. By comparing the concepts, it was possible to unearth nuanced differences across the concepts and categories. One category of respondents may perceive *"concern for safety of finances*" as highly sensitive and another perceived it as less sensitive. Table 6.2 below presents the main points of the coding in this section.

Table 6.2: Summarises how varying privacy categories perceive information differently in this section.

Factor	Open and Axial coding		**Induction (Selective coding)**
	Category (Types of concern)	**Subcategory (Dimensions across PG, PP and PU)**	
Users Economic Status from High Income Group	Concern for identity	**HI-PG:** Perceive identity information as highly sensitive	Implications of perceiving information as highly or less sensitive
		HI-PP: Perceive identity information as highly sensitive (except moderated by benefits)	
		HI-PU: Perceive identity information as highly sensitive (except moderated by lack of agency)	
	Concern for safety of finances	**HI-PG:** Perceive financial information as highly sensitive	
		HI-PP: Perceive financial information as highly sensitive	
		HI-PU: Perceive financial information as highly sensitive (except moderated by benefits)	

6.2.1. The Impact of Incomplete Information and Cognitive Limitation

One of the main concerns when using the smartphone is with apps capturing purchases that most respondents across the 3 privacy categories fear will enable companies to ***profile them***. These sets of concerns represent the impact of incomplete information and cognitive limitation as respondents do not have full information about how the collected information will be used. The concepts relating to profiling emerged when this researcher asked: "Do you have privacy concerns when you use your smartphone online?" This respondent replied:

> *"One of my worries is with apps collecting information on things I buy and knowing where I buy them from. I am concerned because they are able to monitor what I buy and could easily create a profile of my income and other things".* HI-PG 01

Also, another HI-PG 02 said: "*I don't use store apps to collect points from purchases I think it's a way of collecting my information and guessing into my finances*". This phenomenon was confirmed again when another HI-PG 03 said*: "If they know your financial worth, they will flood you with targeted advertisements. I am not comfortable with this".*

The concern for ***status profiling*** is strong among high-income privacy guardians. This concept emphasised the importance such individuals place on preserving their relative social or professional position from being a public knowledge.

The concern for *status profiling* was also found among the HI-PP. This emerged when this respondent said:

> *"When businesses or those who collect our data can build a true profile of the person, they have succeeded in putting us into a market segment. This is a concern to me if its exact and exploits me or discriminates against me".* HI-PP 08

In addition, this concern was revealed when another HI-PP 09 said: "*I am slightly concerned with giving out descriptive information about myself*". On the other hand, other HI-PP revealed contrasting views. This came out when this HI-PP 11 said*: "my smartphone can tell lot about me, however the benefit to me is more, so I don't bother much about things like being profiled".*

From these example statements, the concern for *status profiling* also exists among

some high-income privacy pragmatists, but the benefits of using the smartphone seem to moderate the effect in some cases. Therefore, this concern is not strong among the HI-PP like among the HI-PG group.

High-income privacy unconcerned (HI-PU) also perceive *status profiling* as a privacy concern due to lack of agency. For example, this respondent gave some reasons for this concern:

> *"Information about my status allows data collectors to predict who I am. Such classification can affect my transactions negatively through price discrimination. But I don't worry so much about privacy because there is not much, I can do about it*". HI-PU 17

Another respondent made connections between status profiling and identity theft. *"When your status is known, and it is of interest to them* [data collectors], *your information becomes a target for marketing or fraud. One's complete identity becomes the next target."* HI-PU 18. From this respondent's discourse, it is shown that *status profiling* is perceived by HI-PU as a step towards identity theft.

The concern ***for security of identity*** has been revealed among the 3 privacy categories of high-income smartphone users. This emerged when the researcher asked: "*what has been your experience with an improper invasion of privacy through your smartphone phone?"*. This respondent replied:

> "*I have been so lucky that I haven't had people hack my phone but my main concern in this regard is how I can use the smartphone and not have to worry about my identity been hacked because I am aware the phone knows so much about me".* HI-PG 04

Furthermore, the following respondents said: *"keeping my identity safe is my greatest worry".* HI-PG 05

> *"Identity theft still remains one of my main concern with using he smartphone. The phone carries a lot about me, and it is my wallet also. It is scary to think of this. If my phone is hacked, they can almost get everything about me, so that's my main worry."* HI-PG 07

In addition, high-income privacy pragmatist (HI-PP) are concerned about ***security of identity,*** but it is moderated by benefits. As an example, these respondents said:

> *"I have privacy concerns when I use my smartphone online. I am sure that people are gathering personal information of mine*

and using it for reasons that I do not understand. But I think it's a give and take situation". HI-PP 09

"Identity and behaviour are the key information at risk. Although I am concerned about that, I do not think there is a lot I can do about it. […] so, I will disclose if necessary". HI-PP 10

The phrase: "…*I am sure that people are gathering personal information of mine and using it for reasons that I don't understand…"* clearly shows the impact of incomplete information and/or cognitive limitation to understand privacy notice that provides the information about how personal information collected will be used.

Similarly, HI-PU worry about the security of identity. For example, this emerged clearly when this respondent said: *"when I am using my phone on the internet, I am scared that somebody can access my profile and also see what I am writing or saying and get to know my identity."* HI-PU 19

Other HI-PU feel there is nothing they can do to protect their identity due to invasive technologies, suggesting the ***lack of agency***. This was clear when one respondent said:

"I have concern, but I don't overly think about it, I tend to think that there is not much I can do about it, technologies have made this so easy, so I don't want to be worried all the time". HI-PU20

These concepts ***concern for profiling, concern for identity*** and a ***lack of agency*** emphasised the importance of either protecting or the inability to protect user-identity in the minds of high-income smartphone users across the 3 privacy categories. The varying level of concerns across the different participants indicate how economic status may be a factor shaping the perception regarding identifying information. These emerged concepts are useful and provides the basis for another round of interviews that seeks to unearth how respondents connect these privacy concerns with their economic status.

The emerged concepts are grouped under the *concern for identity category*. HI-PG, HI-PP and HI-PU participants share similarity in perceiving identity information as highly sensitive except in some cases - some HI-PP are influenced by benefits, whereas HI-PU are affected by lack of agency.

6.2.2 Creation of Privacy Zone among High-Income Groups

Privacy zone is defined as the mechanism of building selective boundaries of control that enables individuals to decide which information should stay private (see section 4.4.3). The group of concepts that shows how respondents discriminate between types of information by creating distinctive sensitivity towards specific information suggests the creation of privacy zone. These types of phenomena were revealed among the high-income respondents by continuing the analysis process and using a constant comparative method. This includes the ***concern for safety of finances***. This emerged when the researcher asked: *"what kinds of information in your smartphone or that may be accessed through it are particularly sensitive to you?".* They replied*:*

> *"Financial information. For example, it is much easier to access through your phone because it has become a wallet. If someone gets a hold of my credit card through my phone, then that's a financial risk".* HI-PG 02

This concept emerged again among the HI-PG when they said: *"my smartphone could easily be my identifier; I don't want this connected in any way to my monetary transactions".* HI-PG 07.

Also, most HI-PP are of the view that: "*most hacking target personal details to access people's finances, so this possibility bothers me a lot*" HI-PP 15. Another respondent confirms that: "*my financial transactions are the riskiest information even though I buy things through my smartphone, I am very concerned*" HI-PP 13. Additionally, HI-PU respondents mentioned the safety of finances as a concern with transacting through the smartphone. HI-PU 21 said: "*although I don't bother much about online privacy, I am bothered about my card details being stolen*". To confirm that this was not an isolated view, another respondent said:

> *"Privacy concerns are here to stay with us. So, to keep worrying over it, is to be too concerned because technologies and businesses have taken over our privacy. The one thing I bother a bit about is my financial information and how to secure them."* HI-PU 22

These excerpts describe what high income respondents perceive will be affected if their data is stolen or wrongly used. They are grouped under the concept label ***concern for safety of finances***. This was the label the researcher chose to describe

the information. In addition, the ***perceived worth*** of a company influences high-income users' willingness to disclose their personal information for fear of financial scam. This concept emerged emphatically among HI-PG when asked if it would be risky to give personal information through your smartphone? they said, "*Yes, I feel it's a lot riskier with merchants who are not strong financially.* Reputation is also an issue, *so, I prefer to deal with famous apps owned by financially strong businesses"*. HI-PG 05. Furthermore, "*I feel they are safer as they have a name to protect"* HI-PG 06.

High-income privacy pragmatist (HI-PP) also feel that the reputation or perceived worth of an app publisher is a key factor affecting disclosure. HI-PP 12 said:

> *"when making payment online using my smartphone, I always prefer PayPal because it is big organisation. So, for me, whatever happens to the money, I will get it back."* HI-PP 14

Confirming this point of view, another HI-PP16 adds that: "*I trust big corporations with my personal information more than those nameless ones who have nothing much to lose in terms of public image".*

The concept of perceived worth was de-emphasised among HI-PU when they said: "The *value or benefit that I receive by using the app is the main consideration for me. But I think the general app market can be quite risky because you never know which app can leak your data"* HI-PU 22. In addition, a related concept which the researcher named ***popularity*** emerged:

> *"The willingness to use certain apps by giving your financial information depends on its popularity and how much they have been dependable over time and the level of complaints people have made about it. So, I check reviews before I do anything like buying from an app."* HI-PU 20

These concepts: ***concern for safety of finances***, ***perceived worth and popularity*** (among HI-PU) have been grouped under the *concern for safety of finances category* because they share similarity in properties and dimensions. Like the concern for identity factors, HI-PG, HI-PP and HI-PU participants perceive this category as highly sensitive except in some cases - some HI-PU concerns are influenced by rewards.

These emergent concepts from the high-income smartphone users*;* ***status profiling****,* ***concern for security of identity, lack of agency, concern for safety of finance, perceived worth and popularity****,* have been compared with each other by asking

questions such as: What is this? What does it represent? The questions guided the categorisation of the concepts into two groups: ***status profiling and concern for security of identity*** and ***lack of agency*** are grouped under the ***concern for identity category*** and ***concern for safety of finance, perceived worth and popularity*** are grouped under the *concern for safety of finances category* based on similarities in properties and dimensions. From the first interview, the researcher obtained these first categories that guided further data collection process by applying theoretical sampling and constant comparison methods. From the second and third rounds of interviews, other concepts have been revealed. ***Awareness*** in the minds of high-income users is another concept. This concept emerged when the researcher asked: "How do you relate your income status to your concern for personal information that may be accessed through your smartphone?" This respondent replied:

> *"I am aware that I have a lot at stake financially and so I must remain safe online especially through my smartphone. Because my phone's unique ID and other information can identify me. Then the fact that I don't feel like my phone is very secure is the reason I try to avoid having sensitive information on my phone."* HI-PG 02.

Apart from the HI-PG, this concept emerged also from the HI-PP respondents' speech. For example, ".... *I have concerns about giving my details because of what they can do with it*...". In applying the constant comparison technique, this researcher compared the concept of ***awareness*** with the concepts of ***concern for status profiling*** and ***concern for identity*** that emerged from the first interviews. The comparison reveals that high-income respondents have an ***awareness*** of the financial worth of their personal information. Therefore, a high level of privacy concern is attached to it. Additionally, "*Security issues constitute another problem for smartphone users*." Furthermore, some people had unpleasant experiences that affected trust in mobile apps. This awareness made them to create privacy zone around financial information and were cautious with sharing personal information with genuine requests. They said "*I heard news regarding people's accounts accessed and moneys stolen. So, obviously this affects the confidence to disclose personal information.*" HI-PP12

Similarly, *awareness about real and perceived data breaches* is a hinderance for engaging with mobile apps among the **HI-PU**. This was revealed when they said "*I got experienced. I became aware that the app* is not secure, so I avoided it." And

says in a different place: "*I prefer buying from eBay using my phone, because I usually receive discount offers, making it cheaper online than buying directly from the shops.*" HI-PU 17.

These concepts emphasise the importance of *awareness* in the minds of high-income smartphone users about financial information. The concept is grouped under the *concern for safety of finances category* as the perception of awareness in this context relates to potential monetary loss if a user suffers privacy breach.

6.2.3 Influence of Time Constraints among High Income Group

Confidence and trust are products of adequate processing of relevant information (Dinev and Hart, 2006; Xu et al., 2011b). When respondents say they lack confidence, it suggests the of lack adequate time to process relevant information. Therefore, this type of phenomenon is attributed to constraints of time. The concept of ***confidence*** was uncovered from different respondents across the HI-PG and HI-PP privacy categories. This was clear when this HI-PG said*:*

> *"The main issue is time to read the privacy notices. Not knowing the disclosure terms cause the fear of using the smartphone to buy anything because it has a vast amount of my personal information that can give away a lot of things that have economic value to me. I really need more confidence to use it"* HI-PG 06

The phrase: *"…The main issue is time to read the privacy notices…"* raises the issue of finite amount of time. Suggesting that without this limitation, information seeking response should take place. This shows that high information sensitivity could lead to information seeking response. Conversely, HI-PP respondents said "*…when people do not have the time to read this long notice and obviously, they are* ***not confident*** *to disclose personal information.*" HI-PP 12 And *"I am not really confident using these apps; I really don't know what information of mine they are taking but I still need to use the apps anyway."* HI-PP 14. This highlights the necessity of putting a strategy in place that will reassure pragmatist users of privacy through short notices. Since "***need for confidence***" shares similarity with "***awareness****"* in its properties and dimensions, they are grouped in the same *concern for safety of finances category.*

This researcher categorised all the concepts that share properties into one category. These categories are *concern for identity category and concern for safety of finances*

category. The *concern for identity category* has the role of identity-protection concept. This phenomenon has a considerable influence on individuals' decision to provide their personal information through the smartphone and to engage with apps.

Concern for identity factors raise the perceived sensitivity for identifying information that reveals economic status, whereas *concern for safety of finances* raises users' perceived sensitivity for financial information. This is because financial information signposts a user's economic status. However, the phenomena differ from one privacy concern category to another. The HI-PG category think that identity can be easily stolen and are overly sensitive and suspicious about it. Therefore, HI-PG perceive identity information as highly sensitive. Likewise, HI-PP participants perceive identity information as highly sensitive except when their sensitivity is influenced by *benefits*. Under such influence, HI-PP could trade identity information for perceived benefits unlike the HI-PG. Additionally, HI-PU participants perceive identity information as highly sensitive except when influenced by lack of agency.

The *concern for safety of finances category* includes the concerns of individuals about the potential misuse of personal information to fraudulently access their money. HI-PG like the HI-PP participants perceive financial information as highly sensitive. However, HI-PU also perceive financial information as highly sensitive except when sensitivity is influenced by *benefits* such as rewards. To illustrate the differences and similarities in the cause/consequence paths leading to the differences in perceived information sensitivity among the different categories of users, table 6.3 below present the concepts from the open coding stage among the high-income respondents.

Table 6.3: Emerged concepts from the open coding stage from the HI-income perspective.

HI-PG	HI-PP	HI-PU
Status profiling	Status profiling	Status profiling
Security of identity	Security of identity	Security of identity
Concern for safety of finances	Concern for safety of finances	Concern for safety of finances
Awareness	Awareness	Awareness
Confidence	Reputation	Popularity
Perceived worth	Benefits	Lack of agency

The next stages of analysis are the axial and selective coding to discover the core category that encompasses the identified categories. To do this, the researcher put back data together to make connections between categories in the axial coding process. This happens through a *paradigm model* which is a coding guide – *see 5.3 and figure 5.1* – that makes the analysis process stronger. From the open coding stage, two categories emerged: the *concern for identity factors and concern for safety of finances categories.*

The two categories which are *concern for identity and concern for safety of finances categories* have similarities which led the researcher to apply the paradigm model to connect them together. For example, let us review what has been said by some respondents about *concern for identity category* that influences the perception of information sensitivity. This respondent said, privacy is one of the main concerns of users when using the smartphone online: "*I am concerned because they are able to monitor what I buy and could easily create a profile of my income and other things* HI-PG 01", which suggests that privacy and security of identity constitutes problematic issues for high-income smartphone users. Table 6.4 below illustrates the nodes/themes developed through the open/axial/selective analytic procedure.

Table 6.4: The nodes/themes developed through the open/axial/selective analytic process from HI respondents

Open codes/nodes	**Axial codes/nodes**	**Selective code/node**
Status profiling: *"I am concerned because they are able to monitor what I buy and could easily create a profile of my income and other things."* **Security of identity*:*** *"keeping my identity safe is my greatest worry"* **Lack of agency:** *"I have concern, but I don't overly think about it, I tend to think that there is not much I can do about it…"*	**HI concern for identity factors category**	**HI privacy concern *for safety of finances* and *identifying information***
Concern for safety of finances: *"Financial information. For example, it is much easier to access through your phone*	**HI concern for safety of finances factors category**	

because it has become a wallet" **Perceived worth:** *"I prefer to deal with famous apps owned by financially strong businesses."* **Popularity*:*** • *"The willingness to use certain apps by giving your financial information depends on its popularity and how much they have been dependable over time…"* **Confidence:** *"I am not really confident using these apps; I really don't know what information of mine they are taking..."* "*…when people's do not have the time to read this long notice obviously, they are not confident to disclose personal information* **Reputation:** • "…*I feel they are safer as they have a name to protect."* **Awareness:** • "*.... I have concerns about giving my details because of what they can do with it..."* **Benefits:** *"… I really don't know what information of mine they are taking but I still need to use the apps anyway".*		

Through applying the paradigm model, the researcher can induce that the central theme in this situation is *privacy concern*. This results in the *concern for safety of finances*. The respondent says that "*Financial information, for example, is much easier to access through the smartphone. So, I personally try to avoid some apps before someone gets a hold of my credit card through my phone*". The respondent adds that the extent of ***awareness*** is another trigger of privacy concern because being aware of data breach creates the perception of data-insecurity. This emerged when they said: *"I am aware that I have a lot at stake financially and so I must remain safe online especially through my smartphone. Because my phone's unique ID and*

other information can identify me…" Therefore*, concern for safety of finances* category connects to *concern for identity factors'* category. Consequently, the core category is - *concern for safety of finances* and *concern for identity factors*, resulting in perceiving information as highly sensitive among high-income participants. The next subsection will continue the analysis among the middle-income users.

6.3 The Influence of Economic Status from the Middle-Income Group

The earlier section discussed the implementation of grounded theory within the high-income smartphone users across the 3-privacy concern categories. This section discusses the results from the middle-income respondents. The coding process described in subsection 6.2.1 is followed among the middle-income (MI) group. Table 6.5 below shows the main points from the coding in this section.

Factor	Open and Axial coding		**Induction (Selective coding)**
	Category (Types of concern)	**Subcategory (Dimensions across PG, PP and PU)**	
Users Economic Status from Middle Income Group	Concern for identity	**MI-PG:** Perceive identity information as highly sensitive	Implications of perceiving information as highly or less sensitive (discussed in chapter seven and eight)
		MI-PP: Perceive identity information as highly sensitive.	
		MI-PU: Perceive identity information as less sensitive	
	Concern for safety of finances	**MI-PG:** Perceive financial information with higher sensitivity	
		MI-PP: Perceive financial information as highly sensitive (fabricates information)	

		MI-PU: Perceive financial information as less sensitive (influenced by benefits)	
	Incentives	**MI-PU:** Perceive information as less sensitive (Uses *experience* to receive benefits)	

6.3.1 Creation of Privacy Zone among Middle Income Group

The concepts in this subsection shows how participants create privacy zones by discriminating between types of apps and personal information. These concepts were revealed when the researcher asked all respondents this question: "Do you have privacy concerns when you use your smartphone online?" one **MI-PG** replied:

> *"Initially, I had great concern about giving my details to even some useful apps but when I regularly started using lots of apps, especially the more popular ones, I got the experience with how not to give my real details. I became aware also if the apps were secure or not by using some tools like ZAP [**Zscaler Application Profiler**]. So, before I completed a transaction, I would check if the app is secure or not and recently, I installed an app I had not seen before, but I checked that it was a bit secure not to leak my device or financial information to 3rd parties."* MI-PG 23

The careful examination of the above text revealed several concepts. "***Experience***" in using the device is an important influencer of the perception of information sensitivity. This concept was revealed when the respondent said: "*… I got the experience with how not to give my real details" thus suggesting that* users who perceive information as highly sensitive are likely to mitigate privacy risk through information fabrication. In addition, the ***perceived worth*** of a company influences middle-income users' perception of information sensitivity because of the concern for financial fraud. Like HI-PG, this concept emerged among MI-PG when asked if it would be risky to give personal information through your smartphone? they said, "*It is safer to deal with financially strong business because I feel they have better information security systems"* MI-PG 24 and, "*bigger companies come under more*

regulatory scrutiny about data handling, so I feel they are comparatively more secured" MI-PG 28.

Other concepts were revealed from respondents' speech. These concepts show the concerns that middle-income privacy guardians have towards their privacy, when they said, "…*but I checked that it was a bit secure not to leak my device or financial information to 3rd parties."* and added "…*I became* ***aware*** *if the app was secure or not by using some tools like ZAP…",* MI-PG 23, suggesting a *higher concern for safety of finances*. Some MI-PG respondents' data were stolen before as they said: "*my details were stolen, and some money was taken from my card which was saved in the smartphone*" MI-PG 25, so they are not confident with buying through the smartphone. However, *product offer and discounts are attractive incentives to the* MI-PG. They said: "*experience is important because I don't always give truthful information*" MI-PG 27. And another said: "*I prefer buying online which I do more often with my smartphone because its handy and some apps have cheap offers*" MI-PG 26. Therefore, ***incentives*** as a concept emerged from this statement.

Similarly, the concept of *experience* was uncovered among **MI-PP** respondents which affects their judgement. This came out when they said: "*I use my phone regularly and I can say I have valuable experience to judge when to disclose personal information. One will have to disclose this information at some point if we must use the smartphone*" MI-PP 29. Also, MI-PP 31 adds that *lack of experience* with the smartphone and apps settings is another problem because users should know how to block or allow collection of personal information by apps. This emerged when they said,

> "*this is important because the user who does not know the kind of app, he is going to deal with can lose vital information. I think familiarity with the device and apps should guide the user. For me, it depends on what I want to do with the apps"* MI-PP 31.

A set of strategies could be set in place to support this issue, by emphasising the importance of experience in the minds of users and enabling them to protect their information through the device and apps settings. Otherwise, data collectors could take users' personal information without giving anything in return. However, they said based on experience, "*some apps are trustworthy, and users are re-assured about their information privacy. This provides comfort to disclose relevant information"* MI-

PP 23. Conversely, *experience* is not used to protect personal information among the MI-PU**.** They said, "*I have experience with my phone and apps settings, but I don't bother about blocking the background operations of apps.*" MI-PU 32 Another said: "*I use lots of apps for their convenience and* ***benefits*** such as buying through *my smartphone*" MI-PU 34.

Additionally, ***stereotyping*** about apps emerged when they said: "there *are apps you should trust and some that you should not because they just look fraudulent"* MI-PU 33*.* Among the MI-PU, use experience to create stereotypes. Therefore, stereotyping replaces experience as information protecting concept. From continuing the analysis process as explained in chapter five, several concepts have emerged from the respondents' discourse, namely: ***experience, perceived worth, awareness, stereotyping, higher concern for safety of finances, benefits, and lack of experience.***

The phenomena differ from one privacy concern category to another. For example, MI-PG use *experience* to protect personal information because they perceive information as highly sensitive. Conversely, MI-PP and MI-PU use *experience* to receive benefits, because they perceive information as less sensitive compared to MI-PG. Also, some MI-PU use *stereotyping* to judge apps instead of *experience.* To illustrate these differences, table 6.6 below present emerged concepts from the open coding stage among the middle-income respondents.

Table 6.6. Emerged concepts from the open coding stage from the MI-income perspective

MI-PG	**MI-PP**	**MI-PU**
Experience	Experience	Stereotyping
Perceived worth	Lack of experience	Benefits
Awareness		
High concern for safety of finances		

In the next stage of axial coding, this researcher categorises all the concepts that have similar properties into one category. These categories are *concern for identity and concern for safety of finances. Concern for identity factors* support the protection of identifying information that could reveal users' economic status, whereas *concern*

for safety of finances show how users directly protect financial information. Financial information signposts a user's economic status.

The *concern for identity factors category* covers the role of ***experience, stereotyping,*** and ***lack of experience*** and the *concern for safety of finances category* encompasses the concepts of ***higher concern for safety of finances****,* ***Perceived worth*** *and* ***awareness****. A*nother category, *incentives* which shows how benefits influences the other categories was uncovered*.* This phenomenon influences people to withhold or disclose personal information through the smartphone. Some users are more aware of potential risks that restrains truthful disclosure whereas others are inclined to the benefits of disclosure that makes their life easier. Table 6.7 below summarises the emerged codes and categories from the open, axial, and selective coding analytic procedure among the MI respondents.

Table 6.7: The nodes/themes developed through the open/axial/selective analytic process from MI respondents.

Open codes/nodes	**Axial codes/nodes**	**Selective code/node**
Experience: *"when I regularly started using lots of apps, especially the more popular ones, I got the experience with how not to give my real details."* *"…I can say I have valuable experience which I use to judge when to disclose personal information"* ***Stereotyping:*** "there *are apps you should trust and some that you should not because they just look fraudulent"* ***Lack of experience:*** *" the user who does not know the kind of app he is going to deal with can lose vital information"*	***MI concern for identity factors category***	*Higher concern for safety of financial information* and *concern for identity factors* are moderated by benefits of using the device.

Higher concern for safety of finances: *"sometimes the risk involved in disclosing personal information may be negligible, as long as my identity and other valuable is not stolen"* *"Can we really protect our personal information? I strongly doubt it. When big organisations fail to do so?"* ***Awareness:*** *"my identity is very important to me, if my transaction is known without knowing who is behind, I am comfortable"* *"my identity is important, but the risk is overexaggerated"* ***Perceived worth:*** *"It is safer to deal with financially strong business"* *"bigger companies come under more regulatory scrutiny about data handling"*	***MI concern for safety of finances factors category***	
Benefits: *"I look out for any benefit in the request such discounts and rewards that gives me money somehow".* *"I have bought products that I realized I didn't"*	***Incentives***	

The next stages of analyses are the axial and selective coding to discover the core category that include all the other categories found. From validating and filling the gaps between categories to find an all-encompassing category, the emerged category from the axial coding stage are ***middle-income-users' privacy concerns for identity factors category, safety of finances factors category, and incentives.*** In the selective coding process, the core category that emerged is - *higher concern for safety of financial information* and *concern for identity factors* are

moderated by benefits of using the device. The next subsection will continue the analysis among the low-income users.

6.4 The Influence of Economic Status from the Low-Income Group

The earlier sub-sections 6.2.1 and 6.2.2 discussed the implementation of grounded theory within the high- and middle-income participants across the 3-privacy concern categories. This sub-section implements the GT procedures within low-income (LI) group across their 3 privacy categories. This helps to discover the concepts that reveals the influence of low-income status on how distinct participants perceive information. Table 6.8 shows the coding process and previews emerged concepts.

Table 6.8 showing the coding process and previews emerged concepts.

Factor	Open and Axial coding		**Induction (Selective coding)**
	Category (Types of concern)	**Subcategory (Dimensions across PG, PP and PU)**	
Users Economic Status from Low Income Group	Low concern for security of identity category	**LI-PG:** Perceive identity information as highly sensitive	Implications of perceiving information as highly or less sensitive (discussed in chapter seven)
		LI-PP: Perceive identity information as less sensitive (moderated by benefits)	
		LI-PU: Perceive identity information as less sensitive (moderated by lack of agency)	
	Low perception of financial risk category	**LI-PG:** Perceive financial information as less sensitive	
		LI-PP: Perceive financial information as highly sensitive (fabricates information)	
		LI-PU: Perceive financial information as less sensitive (lack of agency)	

Like high-income and middle-income respondents, low-income respondents expressed concern about apps (store reward cards/apps) capturing purchases which could ***profile them***, as profiling may lead to price discrimination and identity theft. This was explicit when the researcher asked: "Do you have privacy concerns when you use your smartphone online?" this respondent replied:

> *"I am concerned about the recording of the things I buy. This gives away my spending pattern and obviously my income status. This information could be linked to other data to infer my identity".* LI-PG 37

6.4.1 The impact of incomplete information and cognitive limitation

The underlying reasons for the type of concerns raised by LI-PG 37 above reflects the impact of incomplete information and cognitive limitation. This results from not having complete information and/or understanding of how the collected information will be used. Furthermore, LI-PG 38 said:

> "*I am concerned about collecting store or reward points as this creates my purchase profile which can be used to guess my identity when they combine it with other information such as my name and phone number used to create the account".* LI-PG 38

This phenomenon was confirmed when another LI-PG 41 said*: "the type of things that I purchase, and the frequency of purchases could reveal my financial worth. I am not comfortable about this".* The concern for ***status profiling*** is equally strong among LI-PG. These concepts emphasised the importance LI-PG participants place on preserving identity, relative social and financial status from being exploited for marketing.

The concern for *status profiling* was also found among the LI-PP. However, the concern seems to be moderated by perceived benefit. This emerged when the respondent said:

> *"I use store cards and apps. Although I am concerned that my expenditures and preferences are recorded, the extra bonuses I receive makes up for me. I don't have anything to hide."* LI-PP 42

Similarly, another LI-PP 44 said: "*I am not too concerned with giving my information in shopping reward apps like Nectar* [a store reward app] *which I use*". And *"I could*

receive discounts up to 20% so, in such instance, I will give my details. They usually ask for name, email, and phone number." LI-PP 43. Furthermore, these respondents said: "*most people provide their information because they think nothing will happen to their profile and identity or that we most times do not really bother about what we cannot control"* LI-PU45 and *"I don't think my personal information is worth much to them"* LI-PU 47.

Another phenomenon, ***weak concern for security of identity*** which shares similarity with status profiling has been uncovered by these respondents' discourse. From these discourses, low-income participants perceive as less sensitive the information that enables *status profiling*.

Other low-income respondents confirmed that concern for ***security of identity*** has weak effect across all low-income groups. For example, when the researcher asked what is the information that is most sensitive to them and that may be collected through the smartphone? This LI-PG 35 said: "*It is my card details. Next to it is my identity. However, I use my identity details to receive discount when I have to".* In addition, the weak concern for security of identity was clear when they said: *"Sometimes the risk involved in disclosing personal information may be negligible"* LI-PP 43. A*lso, "can we really protect our personal information?"* LI-PP 44.

The above concepts revealed how different low-income participants perceive information regarding ***security of identity***. The concepts also reflect how incomplete information and cognitive limitation allow some respondents to perceive information as less sensitive compared to respondents in higher income groups. For example, they said: "*most people provide their information because they think nothing will happen to their profile and identity…"* LI-PU45.

The various concepts are grouped under the *low concern for security of identity category*. In continuing the analysis, some respondents say they are unable to protect personal *information*. They said: *"can we really protect our personal information when big organisations fail to do so?"* LI-PU 44*.* From this respondent's discourse, it is revealed that *status profiling* and identifying information are perceived by LI-PU respondents as unprotectable due to *lack of agency.*

Other phenomena have been uncovered among the low-income groups when they answered the question: "would it be risky to give personal information through your

smartphone? Two phenomena emerged: ***low concern for safety of financial information*** and ***low value for personal information*** which were grouped under the l*ow perception of financial risk* category because they share similarities in its properties and dimensions. Both phenomena were clear when LI-PG 37 said: "*there is not much they can get from me, so I don't bother much about financial information"*. The same phenomena cut across LI-PP and LI-PU. This was explicit when this respondent said:

> *"There are always risk with everything we do in life, so it's not different when I have to use my financial information for transactions through the smartphone. We just have to live with the risk"* LI-PP 43

And when they said:

> "*one cannot refuse disclosure of financial information all the time and be able to purchase, so we must take the risk and expect nothing will go wrong*" LI-PU 44.

From these statements, the reason for the lower concern for financial risk is the feeling of *lack of agency* about the protection of financial information: "*we just have to live with the risk"* LI-PP 43*.* However, a first-hand experience of financial data breach results in high concern for financial information. This came out clearly when this respondent said: *"…I mind what I do with my card details on the device as my card details were stolen before".* The respondent further explained that: *"I am now very protective of my financial information"* LI-PP 42. This type of perception stands out from the rest LI-PP respondents.

These emergent phenomena, concern for *status profiling, weak concern for security of identity, lower value for personal information, lower concern for financial information* and *lack of agency* have been compared with each other by asking the questions: What is this? What does it represent? Therefore, phenomena that share properties have been grouped into the same category. Two categories are characterised: *low concern for identity factors* and *low perception of financial risk factors****. Status profiling***, ***weak concern for security of identity*** and ***lack of agency towards identity protection*** are grouped under the low *concern for identity category*, whereas ***low value for personal information*** and ***low concern for financial information*** and ***lack of agency towards financial information*** are grouped under the *low perception of financial risk factors category.*

From the first interview, the researcher obtained some initial concepts that guided further data collection. In the subsequent interviews, other concepts were revealed such as ***higher influence of rewards***. This emerged when the researcher asked: "*what other factors will influence you to disclose personal information through your smartphone?*" and this respondent replied:

"If there are benefits in the request such as discounts and rewards that gives me some money somehow, I may give" LI-PG 38.

And *"I have bought products that I realised I didn't even need because of discount offers"* LI-PG 41.

The above excerpts suggest that low-income privacy guardians (LI-PG) behave differently to high-income (HI-PG) and middle-income guardians (MI-PG) about the ***influence of rewards.*** In addition, the phenomenon of ***low value for personal information*** was confirmed when some LI-PP and LI-PU gave the reasons for the higher influence of rewards when they said: "*I have nothing to hide personally, so one may not be too bothered*" LI-PU 47, because *"I don't think my personal information is worth much to them"* LI-PU 45.

The phenomenon of ***higher influence of rewards*** is grouped under the *low perception of financial risk category* because it shares similarities in its properties and dimensions with other *factors in the* category.

At this point, the researcher began the axial coding of the emerged categories from the low-income respondents. Two categories emerged: the *low concern for identity factors* and *low perception of financial risk categories*.

The low *concern for identity factors* and *low perception of financial risk categories* have similarities hence the researcher applied the paradigm model to connect them. Connecting them requires reviewing what was said. For example, "*If there are benefits in the request such as discounts and rewards that gives me some money somehow, I may give"* (LI-PG 38), which shows that incentive is a major moderator of privacy concern among low-income participants.

Applying the paradigm model revealed the central phenomenon that ***privacy concern is moderated by perceived benefits and lack of agency.*** This suggests that a set of strategies could be formulated to challenge this issue, by pointing users to the risks involved in giving away personal information and empowering them to overcome lack of agency. Otherwise, such users could be exploited, as they said: *"I*

have bought products that I realised I didn't even need because of discount offers" LI-PG 41.

To focus the analysis, concepts were sorted into subcategories in table 6.9 to show how concepts emerged from the different participants. It illustrates that all low-income privacy categories have similar results. This shows that privacy attributes have weak effect among them.

Table 6.9. Emerged concepts from the open coding stage from the LI-income categories.

LI-PG	**LI-PP**	**LI-PU**
Higher influence of rewards	Higher influence of rewards	Higher influence of rewards
Weak concern for security of identity	Weak concern for security of identity	Weak concern for security of identity
Low concern for safety of financial information	Low concern for safety of financial information	Low concern for safety of financial information
Low value for personal information	Low value for personal information	low value for personal information
Status profiling	Status profiling	Lack of agency
	Perceived benefit	Perceived benefit

To illustrate the analysis, the codes developed throughout the open, axial, and selective coding analytic procedure among the LI respondents are presented in table 6.10 below.

Table 6.10: Presents the codes/nodes from the open, axial, and selective coding procedure from LI respondents.

Open codes/nodes	Axial codes/nodes	Selective code/node
Status profiling (weak): *"if my transactions are known I am comfortable,"* ***Lack of agency towards identity protection:*** *"Can we really protect our personal information? I strongly doubt it. When big organisations fail to do so?"* ***Weak concern for identity:*** *"sometimes the risk involved in disclosing personal information may be negligible,"* *"my identity is important, but the risk is overexaggerated."*	***Reduced concern for identity***	***Perceived benefits* and *lack of agency are moderators of privacy concerns among low-income users.***
Lower concern for financial Information: • *"I do not have much at stake financially, so I am not really bothered…,"* • *"there is not much they can get from me, so I don't bother much about financial information,"* ***Lack of agency towards financial Information:*** *"There are always risk with everything we do in life, so it's not different when I have to use my financial information for transactions through the smartphone or anywhere online. We just have to live with the risk"* ***Lower value for personal Information:*** • *"I have nothing to hide*	***Lower perception of financial risk***	

personally, so one may not be too bothered" *" I don't think my personal information is worth much to them."* ***Higher influence of benefits:*** *"I look out for any benefit in the request such discounts and rewards that gives me money somehow"* *"I have bought products that I realised I didn't even need because of discount offers"* *"I will disclose if they offer any thing with monetary rewards"*		

The next stage of analysis is the axial and selective coding to discover the core category. From validating and filling the gaps between categories, the emerged categories from axial coding are the r*educed concern for identity, lower perception of financial risk*. However, the core category from the selective coding process is *perceived benefits* and *lack of agency are moderators of privacy concerns among low-income users.* The overall results across all categories shows that privacy guardians perceive information with as highly sensitive whereas privacy pragmatist and privacy unconcerned users perceive information as less sensitive.

6.5 The Influence of Location Tracking From the 3 Privacy Categories

The earlier sub-sections discussed the implementation of grounded theory based on the influence of economic status on the perception of information sensitivity across privacy concern categories. In this subsection, figure 6.3 illustrates the coding processes in this section and the next (section 6.6). It illustrates that text are coded into concepts when respondents mention or imply the effect of location tracking (LT) or app permission request (APR). In addition, if the same concept emerges across the user-categories (PG, PP and PU), the emerging concept is compared across the user-categories. This help to find the influence of location tracking from the privacy categories. Additionally, the concepts that are influenced by constructs from the theoretical framework are grouped together for further discussion (see section 7.6).

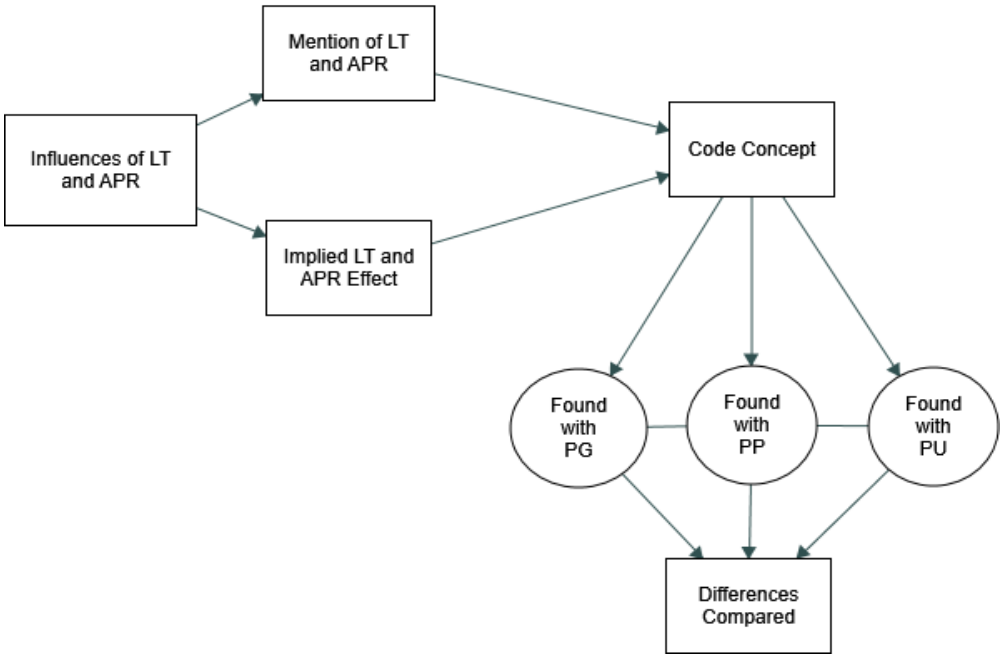

Figure 6.3 illustrates the coding processes for Location Tracking and App Permission Request.

6.5.1 The influence of bounded rationality regarding location tracking

The following concepts reflect the impact of bounded rationality due to its suboptimal decision outcome (Simon, 1982). Location tracking as shown in the following analysis causes varying perceptions of vulnerability. Vulnerable users are most likely to make suboptimal privacy decisions which reflects the outcome of cognitive limitation and incomplete information (Jens et al., 2014; March, 1978).

The effect of location tracking on the perception of information sensitivity among the PG came out from respondents' discourse when they answered this question *"Do you have privacy concerns when you use your smartphone online?"* two phenomena emerged: ***perception of vulnerability*** and ***user-profiling***. Both phenomena were clear when this respondent said:

> *"Yes, I have privacy concerns when I use my smartphone online. Location tracking is a huge concern because from there you can track secondary information about the person. For example, if you go to the same place every day, they can know that is the place you work or where your home is or where your friends are, even where your kids go to school without ever sharing that information."* PG 07

The Straussian procedures were applied as discussed in chapter five. From examining the text above, some concepts were revealed concerning location tracking. The privacy risks triggered by location tracking is perceived to affect most aspects of users lives, resulting in ***"user-profiling"*** which is a prominent issue influencing PG users' perception of information sensitivity and engaging with smartphone app. This concept emerged explicitly from the above statement when this respondent said,

> *"…if you go to the same place every day, they can know that's the place you work or where your home is or where your friends are, even where your kids go to school without ever sharing that information".* PG 07

Besides this one, further concepts such as feeling "***vulnerable"*** emerged from the respondent's discourse. These concepts show the PG's concerns toward their Privacy, when they said, "*Just imagine there is a virtual person following you everywhere you go"* PG 03 and added "*This is really a frightening prospect*". Furthermore, the perception of being "***vulnerable"*** to location tracking is discomforting to most PGs which made them deny apps access to their location data. This respondent said,

> *"When your camera app request for your location, they want to add that information to your photo, when you share the photo, you share the information about where that photo was taken, so I denied the app access to my location."* PG 04

Some PG respondents gave the reason for feeling vulnerable. They said: *"a harmless capturing of location data today could leave vulnerabilities open tomorrow"* PG 23. There are concerns about the "***future use of data."*** *"There is an inherent risk of moving from fitness programmes to surveillance"* PG 25.

Similarly, the phenomenon of "***perception of vulnerability"*** and "***user-profiling"*** emerged amongst privacy pragmatist (PP). These concepts were clear when they said, *"I will usually disable the location permission after downloading the app and enable it when I need to use the app for navigation, to avoid apps capturing all my journeys" PP 08.* Another PP gave the reason as concern for ***physical safety;*** *"this makes me feel exposed everywhere because personal data had been stolen from my device before"* PP 10. Similarly, another PP said, *"My identity was used in a bank*

transaction without me knowing, so I am suspicious of exposing any information relating to myself, because one can be vulnerable without knowing" PP 16. Therefore, a first-hand experience of data breach affected these respondents' perception of vulnerability. Additionally, the ***convenience*** that comes with using the smartphone for mapping is a strong factor affecting the disclosure of location information among the PP and PU when they said: "I *need the app to provide direction for me"* PP15 and one PU respondent added "*It is really convenient to use apps like Waze and Google maps for direction"* PU 17. Conversely, PG respondents did not mention the convenience aspect of using navigation apps.

6.5.2 Creation of privacy zone regarding location tracking

The following concepts show the situations influencing the creation of privacy zones around location information across the distinctive privacy categories. They were revealed through concepts such as ***appropriateness***, ***geo-profiling* (*segmentation based on places of frequent visit*),** and ***intrusiveness*** which emerged when the researcher asked respondents this question: are there any situations that could make you share your location information online through your smartphone? Some PG respondents replied:

> *"Yes, there is but, it has to be appropriate. There have been instances where I needed a map to show me location or proximity so then I had to share my location."* PG 23

> *"I will share my location information if it's an emergency. But it is not a thing I really like to do because, tracking my location continuously can give me away as a frequent visitor of a specific pub and that kind of profiling can be used maliciously."* PG 24

"I am not a fan of having location tracking on, on my phone. Because I do not want to be followed. For this reason, I don't have Facebook app installed on my phone." PG 06

"I will give my location data if, for example, I am using GPS app for navigation. After, I will switch it off." PG 40.

The concepts above showed that PG respondents differentiated location tracking from location information requests. They said, *"I am not a fan of having location tracking on, on my phone. Because I do not want to be followed*…" PG 06, however, others feel that location information request should be ***appropriate*** when they said,

"…Yes, there is [privacy concern] but, it [location request] must be proper…so then I had to share my location", and PG 09 added *"why should apps that are not providing location related service want my location information?".*

On the other hand, ***convenience*** moderates the effect of location tracking among the PP and PU. This was explicit when they said, "*the convenience and benefits of using fitness and mapping apps makes up for the creepiness of tracking me since I don't have anything to hide*" PP 29. Also, PU 32 added other benefits to location tracking, "*location tracking can be beneficial as it can be* ***an alibi*** [digital evidence of location] *to prove one's innocence when it matters. Having a history of my movement has obvious benefits*".

Several concepts have emerged from the PG, PP and PU respondents about the effects of location tracking, namely: *perception of vulnerability*, *user-profiling*, *convenience, appropriateness*, *geo-profiling* (*segmentation based on places of frequent visit*), *intrusiveness (unwelcome following), physical safety* and *future use of data.* Table 6.11 below present the emerged concepts from the open coding stage across respondents.

Table 6.11: Emerged concepts on location tracking from the open coding stage.

Privacy guardian (PG)	**Privacy pragmatists (PP)**	**Privacy unconcerned (PU**
Perception of vulnerability	Perception of vulnerability	Convenience
User-profiling	User-profiling	Alibi **(**digital evidence of location)
Future use of data	Convenience	
Appropriateness		
Geo-profiling (segmentation based on places of frequent visit)		
Intrusiveness		

The next step of axial coding that categorises all the concepts that share the same properties into one category. The categories that emerged are *personal factors*, *situational factors*, and *profiling factors*. The *personal category* comprises the

concepts of *perception of vulnerability*, *physical safety, convenience,* and *future use of data*. These phenomena are significant influencers of users' perception of information sensitivity and they equally influence engagement with smartphone apps. However, the effects of the phenomena vary from one privacy concern category to the other. For example, PG users considers location tracking as frightening and thus, are mindful of the future use of the data, while PP users are more pragmatic by managing the effect through disabling and enabling access to location data. However, the effects are strongly moderated by the *convenience* of using location tracking apps among PU users.

The *situational factors category* shows how individuals judge the *proper timing* of location tracking and how *intrusive* it could be when it is perceived as inappropriate. Unlike the situational category, *profiling factors category* has the role of *user-profiling* concept which raise privacy concerns beyond specific contexts when individuals are *geo-profiled* (*segmentation based on places of frequent visit).* Table 6.12 below presents the codes regarding the influence of location tracking from the open, axial, and selective coding analytic procedure.

Table 6.12: Shows the nodes/themes developed through the open/axial/selective analytic process about the influence of location tracking.

Open codes/nodes	**Axial codes/nodes**	**Selective code/node**
Perception of vulnerability: "*Just imagine there is a virtual person following you everywhere you go"* *"My identity was used in a bank transaction without me knowing, so I am suspicious of exposing any information relating to me, because one can be vulnerable without knowing*" ***Physical safety:*** *"…this makes me feel exposed everywhere"* ***Convenience:*** "*It is really convenient to use apps like Waze and*	***Personal Factors***	**Varying personal, situational, and profiling concerns regarding location tracking.**

Google maps for direction" ***Future use of data:*** *"There is an inherent risk of moving from fitness programmes to surveillance."*		
Appropriateness: *"Yes, there is but, it has to be appropriate. There have been instances where I needed a map to show me location or proximity so then I had to share my location"* *"why should apps that are not providing location related service want my location information?"* ***Intrusiveness:*** *"I am not a fan of having location tracking on, on my phone. Because I don't want to be followed"*	***Situational Factors***	
User-profiling: *"Location tracking is a huge concern because from there you can track secondary information about the person"* ***Geo-profiling (segmentation based on places of frequent visit):*** *"Sharing my location information is not a thing I really like to do because, tracking my location continuously can give me away as a frequent visitor of a specific pub and that kind of profiling can be used maliciously."*	***Profiling Factors***	

The next step of analysis is the selective coding to discover the core category that encompasses all the other identified categories. The emerged categories from the axial coding stage – are *personal factors, situational factors,* and *profiling factors*, while the emerged core category, is the "varying personal, situational and profiling concerns regarding location tracking." The next subsection presents the analysis about apps permission request across the 3 privacy concern categories.

6.6. The influence of apps permission requests from the 3 privacy categories

The earlier section discussed the implementation of grounded theory among different categories of smartphone users based on the influence of location tracking on the perception of information sensitivity. Similarly, this section presents the effect of app permission request (APR) on users' perception of information sensitivity.

6.6.1 The influence of bounded rationality regarding app permission request

The analysis shows that app permission request makes PG participants perceive information as highly sensitive by raising uncertainties regarding permission requests. Permission uncertainty results from incomplete information and cognitive limitation. Therefore, the ***consequences of wrong disclosure*** and the ***autonomy of decision making*** are major concerns. These phenomena emerged when the researcher asked respondents: "does apps permission request affect how you feel in terms of information sensitivity? If yes or no how does it make you feel? This respondent said:

> *"What is most important to me is keeping my autonomy and making sure that the decision I make whether I want to share something or not is right".* PG 25

This respondent's statement explains the concept of ***decision-making autonomy*** explicitly, *"my autonomy is also about making sure that it's my decision to share what I want to share and not to be unduly influenced through quick nudges. This is particularly important".* PG 27

The consequences of wrong disclosure and the pressure to make the right decision is a *huge burden (decision burden)*. When they said: "…*those requests call me to make a huge decision that can have profound consequences if it goes wrong"* PG 26. Apps permission request contend with users' decision-making autonomy when the goal of the request is not known as they said, *"I usually think that the user should*

determine what should be shared" PG 28*.* And then "*I think it's the task of the developers and providers to explain why they need certain data"* PG 37*.* This is because, "*that will make the user have much better feeling for what they are actually sharing"* PG 41*.*

From the words of one respondent, the present situation gives data collectors a lot of leverage. *"At the moment, most providers are of the view that the more we collect, the better. So, let us just collect as much as possible"* PG 38. According to PG 39, apps permission requests should be fit-for-purpose:

> *"Again, if I can see that it is something that they don't need I will often restrict apps. Yes, I am willing to disclose personal information, but I need to be able to see the use-case for the data that I am sharing"* PG 39.

App permissions make PG participants perceive information as highly sensitive when the request is unjustified. The analysis shows that unjustified request increases PGs disclosure uncertainty. Uncertainty results from not fully understanding the consequences of accepting permission request, which in turn shows bounded rationality by constraining the full understanding of accepting the request (see chapter 4, subsection 4.4.4). Further interviews to saturate data and the constant comparative method revealed more phenomena that reflects the influence of bounded rationality such as ***unjustified request*** by apps that causes ***lack of trust***. These came out when respondents were asked: "through apps permission request, most apps ask for specific access to users' information needed for functionality. Are you willing to allow access to your personal information? And why? This respondent said:

> *"I don't trust most app requests because they request authorisation for stuff they don't need, so I have been constantly thinking about that myself […] However, I am aware that many apps do invade my privacy and take the information they do not need".* PG 26

According to PG 24*, "It is one reason I do not have lots of apps to avoid giving away too much information in the background".* The above discourse reveals ***apps-avoidance*** as one consequence of unjustified request. And ***lack of trust*** when another respondent said:

> "*I am not confident that apps do not access my information beyond the permissions granted. Because most request do not match functionality, they* [the requests] *don't add up".* PG 41

To address ***lack of trust*** in data request, they said*, "I will want to know more specifically, what kind of information they* [apps] *are collecting without having to read some detailed information"* PP 43*.* From this statement emerged the *quest for specific and concise explanation* of each app request.

6.6.2 The influence of RALC constructs of choice and consent

The exercise of choice and consent in a data request environment reduces the perception of information sensitivity. This is because when users can exercise choices, they feel empowered to protect privacy. Although the perception of control may not be a reality, it does influence the perception of information sensitivity as the following analysis shows. The concepts that emerged from the discourse amongst the PP and PU participants shows the connection between perception of control and the perception of information sensitivity regarding app permissions. For example, while PG feel uncomfortable with handling apps permission requests, PP and PU are happy with the requests. PP 29 said, "*I am quite happy when I see the request…"* and added *"…because that gives me the choice to say no. Some apps now have runtime requests that ask for access when you need to use certain services. So, that choice is something that gives me a sense of control."* PP 31. The concept of ***perception of control*** therefore emerged from the above statement. In addition, the phenomenon came out among PU. One respondent said, *"I appreciate when the apps ask for my permission before using my location information by default. I feel a kind of comfortable with this practice"* PU 32. And to confirm that ***perception of control*** was not an isolated opinion, another respondent said:

> *"But I appreciate they* [apps] *ask and not doing it* [accessing user information] *without asking me. However, when the apps want to access my contact, that is going to be a problem. I don't want somebody having a list of my contacts because an app has stolen my contacts before."* PU 36.

Besides this one, another concept emerged from the respondent's speech. These concepts show PU ***selective concerns*** toward certain information which can be problematic when they said, "…*my emails are very sensitive to me" PU45* and "…*I don't want apps to access my photos, they are very personal to me."* PU 47

The ***selective concerns*** revealed by some PU above (PU 45 and PU 47) which contrasts with the emerging pattern of ***perception of control*** among PU could be

explained by their gender characteristics. Both respondents are female, and studies (Baruh et al., 2017) shows that women are more concerned about privacy than men.

The above concepts emphasised the influence of apps permission requests on different smartphone users' perceived information sensitivity. These concepts are *consequence of wrong disclosure**,** decision-making autonomy, decision burden, perception of control, unjustified request, apps-avoidance, lack of trust, quest for specific and concise explanation*, and *selective/problematic concerns.* The table 6.13 below present example concepts from the open coding stage.

Table 6.13: Emerged concepts from the open coding stage from apps permission request.

Privacy guardians (PG)	**Privacy pragmatists (PP)**	**Privacy unconcerned (PU)**
Consequence of wrong disclosure	Sense of control	Perception of control
Decision-making autonomy	Quest for specific and concise explanation	Selective/problematic concerns
Decision burden		
Unjustified request		
Apps-avoidance		
Lack of trust		

The next stage of axial coding, the researcher categorises all the concepts that share the same properties into one category. These categories are *concerns factors* and *control factors*. *Concerns factors category* has the concepts of *decision burden, consequence of wrong disclosure, decision-making autonomy, unjustified request, lack of trust, apps-avoidance,* and *selective/problematic concerns*. This phenomenon plays a significant role in shaping different users' perception of information sensitivity towards apps permission requests. However, the phenomena have different impacts across the privacy guardians and the privacy unconcerned. For example, the *concern factors* make PG participants perceive information as highly sensitive, whereas the *control factors* make PP and PU participants to perceive information as less sensitive except request to access contact list, emails, and photos.

The control factors comprise the *perception of control* and *quest for specific and concise explanation* concepts. These phenomena represent the comfort the PP and

PU users perceive and what is needed to sustain it. The impact of the phenomena is seen only among the privacy pragmatic and privacy unconcerned users. Table 6.14 below illustrates the codes and the themes that emerged from the open, axial, and selective coding analytic procedure.

Table 6.14: Illustrates the codes/nodes from the open, axial, and selective coding process about apps requests

Open codes/nodes	**Axial codes/nodes**	**Selective code/node**
Consequence of wrong disclosure: *"…making sure that the decision I make whether I want to share something or not is right."* **Decision-making autonomy*:*** *"My autonomy is also about making sure that it's my decision to share what I want to share and not to be unduly influenced through quick nudges. This is particularly important."* **Decision burden*:*** *"…those requests call me to make a huge decision that can have profound consequences if it goes wrong."* **Unjustified request:** • *"…most request do not match functionality, they* [the requests] *don't add up"* **Apps-avoidance:** • *"It is one reason I do not have lots of apps to avoid giving away too much information in the background."* **Lack of trust:** *"I am not confident that apps do not access my information beyond the permissions granted"* **Selective/problematic concerns:** "…*when the apps want to access my contact, that's going to be a problem.*	**Concerns factors category**	***Concerns and perception of control regarding app permission requests***

Perception of control*:* *"I appreciate when the apps ask for my permission before using my location information by default. I feel a kind of comfortable with this practice"* **Quest for specific and concise explanation:** *"I will want to know more specifically, what kind of information they [apps] are collecting without having to read some detailed information"*	**Control factors category**	

The axial and selective coding is the final stage of analysis to discover the core category that can encompass the other two categories. It validates and fills the gaps between the categories. From this, the core category that emerged is *concerns and perception of control regarding app permission requests.*

6.7 Conclusion

The differences in individuals' perception of information sensitivity are better revealed by the analysis of factors that influences how different categories of users perceive information. This chapter has presented the implementation of the grounded theory method discussed in chapter five to reveal how economic status, location tracking and app permission request influence different users' perception of information sensitivity. The theoretical framework helped to structure the chapter by guiding the understanding of the concepts. Various concepts and categories have been revealed. The next chapter will interpret and discuss the findings of the data analysis in more detail.

Chapter Seven

7. Discussion of Varying Perceptions of Information Sensitivity

7.1 Introduction

The aim of this research is to understand the differences in perceived information sensitivity among smartphone users. Doing this provides insight that enables tailored privacy. Consistent with the aim, this chapter provides the discussion of the varying perceptions and categories arrived at from the data analysis in chapter six. In order to understand the context from which the categories were derived, a contextualisation section will initiate the discussion of each category.

The chapter features eight main sections, section 7.1 provides the introduction. Section 7.2 presents the contextualisation and discussion regarding users' economic status that reveals how users' economic status and varying privacy categories shape the perception of information. Section 7.3 contextualise and discusses findings from the factor of location tracking which also shows how location tracking influences varying categories of users to perceive information differently. Section 7.4 focuses on findings regarding app permission request and explains how and why varying privacy categories perceive information due to the influence of permission request. Section 7.5 discusses the influence of bounded rationality and restricted access and limited control theory (RALC) theories. Section 7.6 examine users' sensitivity perceptions through bounded rationality and RALC and provides theoretical explanation of the findings. Section 7.7 presents the middle-range theory for understanding smartphone users' perception of information sensitivity. Finally, section 7.8 presents the conclusion to the chapter.

7.2 The influence of economic status

The emerged categories are *concern for identity and concern for safety of finances*. These show how and why users' economic status influences information sensitivity perception across the privacy concern categories - privacy guardian (PG), privacy pragmatist (PP) and privacy unconcerned (PU) and their economic status (high, middle, and low).

7.2.1 Concern for identity

The data analysis shows that the concern for identity cuts across most participants irrespective of their privacy concern category. However, the concern is moderated by economic status (income level) and privacy concern categories. The literature shows that concern for identity is a source of distress for online users (Jibril et al., 2020; Wang et al., 2017; Zaeem et al., 2017). However, it is unclear how this concern varies among users. The varying levels of sensitivity across the privacy guardians (PG), privacy pragmatist (PP) and privacy unconcerned as well as users' income status is summarised in table 7.1 below.

Table 7.1 A summary of findings regarding Concern for Identity from 3 perspectives.

	High income group	**Middle income**	**Low income**
Privacy Guardian (PG)	High sensitivity from a strong desire to protect social and professional status	High sensitivity. Uses fabrication to mitigate risks	High sensitivity. LI-PG are not motivated by purchase rewards
Privacy Pragmatist (PP)	Lesser sensitivity compared with PG. Some PP sensitivity are reduced by benefits	Sensitivity is moderated by information search to mitigate risk	Low sensitivity. Reduced by rewards from purchases
Privacy Unconcerned (PU)	Lesser degree of sensitivity compared with the PG & moderated by lack of agency	Reduced sensitivity. Moderated by lack of agency & convenience of using the smartphone	Low sensitivity due to lack of agency & perceived low worth of personal data

7.2.1.1. Concern for identity among privacy guardians (HI-PG, MI-PG and LI-PG)

The concern for identity cause PG to perceive information as highly sensitive because they are less influenced by rewards offers from data collectors. Most HI-PG respondents relate their concern for identity with the concern for status profiling. This respondent said:

> *"What is most important to me is keeping my identity and making sure that my profile is not created in a way that can reveal who I am and what I have…." HI-PG 01.*

The phrase: "… *who I am and what I have…"* seems to refer to the users' economic status. Thus, suggesting that economic status is a salient influencer of users' perception of information sensitivity. The high perception of information sensitivity among HI-PGs can also be explained by the interplay between users' economic status, privacy attribute and the smartphone context. For example, they said: *"The smartphone knows many things about me, so I think if users unknowingly give away more information, it can be used to create their profile, and this will affect their privacy*." HI-PG 07. Therefore, HI-PG feel that the smartphone already captures a lot of information about its users. As mentioned, (see chapter 2 sub-section 2.5.1) the influence of users' economic status has not been sufficiently studied in the smartphone context. If HI-PGs are relating the perception of information sensitivity to the capability of the smartphone, then it confirms the importance of investigating the influence of economic status and privacy attributes in the smartphone context.

The literature (Wachter, 2018) confirms that individuals suffer losses such as discrimination from status profiling. An example is the notorious Amazon.com price discrimination of customers profiled on estimated financial worth. This resulted in selling products at higher prices to high economic status customers (Hinz et al., 2011). Therefore, HI-PGs concern can be interpreted to mean that high economic status increases concern for status profiling. Confirming this, another HI-PG respondent explained why HI-PG users are concerned about status profiling. They said HI-PG have more at stake because of their high economic worth. Therefore, they are inclined to protect their profile:

> *"Personal data is attractive to marketers and others primarily because it can give them marketing edge. The more this data can accurately describe real people and behaviours, the more important it is. So, I do not want to be described in great details. I try to conceal information that are very personal to me." HI-PG 02.*

Another reason HI-PGs perceive identity information with high sensitivity is that information could be wrongly used outside the context of disclosure as they do not have full understanding of the disclosure terms. This has a bounded rationality connotation (Simon 1967). HI-PGs say that a leak of identifying information could affect the security of their person and finances, given the possibility of being tracked by the smartphone. This perception makes HI-PG users worry about providing

identifying information. The following respondents said: *"users' identity must be secured if there will be confidence to transact freely over the smartphone."* HI-PG 6 and HI-PG 3 added:

> *"Unfortunately, as we see the value of personal information increasing because of personalised marketing and services, the concern for our identity will remain the main issue. More so that personal financial worth is involved here. This makes it scary"* HI-PG 3.

Consequently, the concern for safety of identity has a considerable influence on why HI-PG perceive information with high sensitivity. Although not specifically referring to high economic status users, Solove (2003) contention seems to explain high economic status user's high sensitivity perception towards identity information. Solove (2003) argue that the system of collection, dissemination, and use of personal information shapes what he calls "architectures of vulnerability," where people are vulnerable to significant harm such as identity theft which is one of the most rapidly growing types of criminal activity (Solove, 2003). This shows that the concern for identity has been a concern to privacy, but we are now beginning to see how these impacts on distinct categories of users. Surprisingly, middle income privacy guardians (MI-PGs) are likely to show higher levels of information sensitivity regarding the concern for identity when compared with HI-PGs. This is inferred as MI-PGs did not only express this concern, but they also used PET (privacy enhancing technology) or said that they falsify their information to mitigate privacy risks. This was revealed when this respondent said:

> *"I have high concern about giving my details to even some useful apps but when I regularly started using lots of apps, especially the more popular ones, I got the experience with how not to give my real details. I became more experienced. Also, I try to verify if the apps were secure or not by using some tools like ZAP* [Zscaler Application Profiler]*."* MI-PG 23

The above statement reveals that MI-PG creates pseudo-identity to preserve their privacy. Linking MI-PG possibly higher level of information sensitivity to the information falsification response seems to suggest that sensitivity levels can reveal users' tendency for information falsification. However, such proposition should be tested. Similar responses were revealed by LI-PG respondents who expressed high

levels of sensitivity through their suspicion of rewards and other incentives offered by data collectors for identity information:

> *"I am concerned about collecting store or reward points as this creates my purchase profile which can be used to guess my identity when they combine it with other information such as my name and phone number, even date of birth used to create the account"* LI-PG 37

"…using the smartphone comes with some worries. Such as the concern of identity theft but some truthful assurance from trusted parties can help" LI-PG 40

The data analysis shows that despite belonging to different economic status groups (income group), almost all PG respondents share high levels of perceived information sensitivity regarding identity information. This means that PG respondents are aware of the privacy risks regarding users' identity in the smartphone context and will require privacy-assured disclosures that are strong and specific enough to mitigate unwarranted disclosure. Privacy-assured disclosure help users reduce the amount of personal data that may be collected by apps (Mousavi et al., 2020). For example, privacy-assurance mechanisms could be applied to increase users' personal control by showing privacy customisation options in smartphone settings (such as disabling location history) or proxy controls through concise privacy statement and assurance seal (Schaub et al., 2017; Zhou et al., 2017).

7.2.1.2 Concern for identity among privacy pragmatist (HI-PP, MI-PP and LI-PP)

Regarding the concern for identity, data analysis shows that privacy pragmatist (PP) of different economic status (HI-PP, MI-PP and LI-PP) perceive identity information as less sensitive compared with the privacy guardians. For example, HI-PP acknowledged that they were slightly concerned about giving their identity when prompted by mobile apps. They said: *"I am slightly concerned with giving out descriptive information about myself."* HI-PP 08. Descriptive information refers to identity information such as users' name, email address, phone number and even addresses. In other instances, concern is reduced by the benefits of using the smartphone. For example, HI-PP 15 said: *"my smartphone can tell lot about me, however the benefit for me is more, so I don't bother much about things like being profiled".* Such responses typify the privacy pragmatist in the literature (see 3.2.3) who will normally weigh the benefits of disclosure against the level of intrusion. This means that HI-PP could be supported with a good use-case for data request.

Like the HI-PP, MI-PP respondents perceived identity information as less sensitive compared with the MI-PG group. Unlike the HI-PP, MI-PP respondents provided insight on how information sensitivity can be moderated by information-seeking response to mitigate risk. For example, *"I will look at the relevant information to judge when to disclose personal information. One will have to disclose this information at some point if we must use the smartphone"* MI-PP 29. And *"some apps are trustworthy; users are re-assured about their information privacy. This provides comfort to disclose relevant information"* MI-PP 30.

The re-assurance referred to by these respondents suggests that relevant information should be provided to enable the right judgement regarding when to disclose identity information. This explains the relevance of the Publicity Principle in RALC theory (see 4.4.3) which proposes that information relevant to disclosure should be known to individuals that could be affected by information handling (Tavani 2008). Furthermore, the data analysis shows that LI-PP participants perceive identity information as less sensitive compared with LI-PG because they are influenced by purchase rewards through the smartphone. For example, *"I am not too concerned with giving my information in shopping reward apps like Nectar [point and reward app] which I use."* LI-PP 42.

LI-PP needs better understanding of the privacy risks involved with trading off identity information otherwise, they could be exploited by data collectors. The plausible reason for the stronger influence of monetary reward among LI-PP is related to how they value identity information (Doherty and Tajuddin, 2018; Group, 2020; Huberman et al., 2005). This is confirmed as they said: "…*the extra bonuses I receive makes up for me. I don't have anything to hide."*

Overall, high-income status has a weaker impact on how HI-PP perceive identity information due to higher influence of rewards. Acceptance of rewards is a privacy decisions weakness that could be exploited (Carrascal et al., 2013; March 1978). To address this, effective privacy support should be designed to strengthen weaknesses in users' preferences. A segmented privacy support that provides pragmatist with better understanding is possible. For example, request should balance benefit and rewards with "privacy facts" that list the types of information and resource the app can access. However, the effectiveness of this mechanism will depend on app

trustworthiness. Studies show that most apps access more information than the request granted (Degirmenci, 2020; Kulyk et al., 2019).

7.2.1.3 Concern for identity among privacy unconcerned (HI-PU, MI-PU and LI-PU)

The data analysis shows that HI-PU participants perceived identity information as less sensitive compared with HI-PG users. Like LI-PU, HI-PU participants have privacy concerns but expressed lack of agency. For example, this respondent said: *"I have concern, but I don't overly think about it, I tend to think that there is not much I can do about it…."* HI-PU17. This statement clearly shows that the presumption of being unconcerned about privacy can be changed by the information disclosure context. A plausible reason for this is that smartphones introduce vulnerability which imposes the concern for privacy of identity information on PU users. The vulnerability from smartphone use confirms the literature that context of information impacts on the perception of information sensitivity and thus influences privacy decision-making (see 2.4.1). This means that HI-PU needs support to protect identity and thus overcome lack of agency.

Looking at the middle-income group, the data analysis reveals that MI-PU smartphone users, like HI-PU users perceive identity information as less sensitive. This is because their perceived information sensitivity is moderated by the convenience of using the smartphone (see table 7.1). MI-PU users like others in the PU category trade short term benefits for privacy protection. This means that they are affected more by immediate gratification because they lack complete information regarding the consequences of unwarranted disclosure. This seems to suggest that the theorised bounds of rationality (see 4.4.4.) do not have the same effect across all categories of smartphone users. Therefore, understanding the varying effects of bounded rationality have significant implications for how different categories of users are supported. This will be discussed further in section 7.6.

The data analysis shows that low-income PU participants (LI-PU) equally expressed low sensitivity towards identity information due to lack of agency arising from perceived low worth of personal information. For instance, these LI-PU respondents said: *"most people provide their information because they think nothing will happen to their profile and identity or that we most times do not really bother about what you cannot control"* LI-PU 45 and *"I don't think my personal information is worth much to*

them [data collectors] LI-PU 47. Therefore, LI-PU do not differ much from MI-PU in terms of expressing lack of agency. However, the difference is the reasons for the lack of agency. Whereas most MI-PU are influenced by convenience, LI-PU are influenced by low valuation of their personal information which can be explained by their low-income status. Personal data are like money, the net worth of people influences how much value they attach to it. Therefore, it is not surprising that low income users value rewards more than personal data (Group, 2020).

The PU (privacy unconcerned) participants from the 3 income groups (high, middle, and low) all expressed lack of agency as the reason for low sensitivity towards identity information. This suggests that perceived inability to protect personal information (lack of agency) can be associated with a user's privacy attribute rather than income status. However, the PG and PP willingness to protect identity information seems to be associated with the interplay of a user's privacy attribute and income status. Table 7.1 illustrates this trend. It can be inferred that users need distinct types of support towards privacy-preserving decisions (Morton and Sasse, 2014; Semanjski and Gautama, 2016). Our data analysis has shown through the varying perceptions of information sensitivity that users of the PU categories require empowerment to take the right action.

Based on the differences in perceived information sensitivity towards identity information, our analysis shows that smartphone users can be characterised into two groups. They are, (1) users that perceive identity information as highly sensitive, who are high-income PG, middle-income PG, and low-income PG, (2) users that perceive identity information as less sensitive who are high-income PP, PU, middle-income PP and PU, low-income PP and PU.

7.2.2 Concern for safety of finances

Regarding concern for safety of finances, the analysis of empirical data shows that participants differ in their expressed levels of information sensitivity across income and privacy concern groups. Table 7.2 below summarises the differences in perceived information sensitivity and why it differs.

Table 7.2: A summary of the analysis regarding the Concern for the Safety of finances.

	High income group	**Middle income**	**Low income**
Privacy Guardians (PG)	High sensitivity as smartphone could be an identifier and wallet (ecosystem)	Higher sensitivity through the fear of financial fraud.	Lower sensitivity reduced by high influence of rewards
Privacy Pragmatist (PP)	High sensitivity and considers financial info as riskiest.	High sensitivity moderated by information search to mitigate risk	Low sensitivity. Decreased by expression of lack of agency
Privacy Unconcerned (PU)	High sensitivity due to concerns about the smartphone ecosystem	Lower sensitivity. Moderated by convenience of using the smartphone	Low sensitivity due to lack of agency and benefits of using the smartphone

The summary contained in table 7.2 above were revealed from the participants' responses in the interviews with them. The following sections discuss the contents of the table in more details.

7.2.2.1. Concern for safety of finances among privacy guardians (HI-PG, MI-PG and LI-PG)

HI-PG expressed high level of perceived information sensitivity towards the concern for safety of financial information because they related the privacy of financial information to the safety of their finances. For example, HI-PG participants mentioned that the smartphone could be an identifier and a wallet. An identifier because smartphones have device IDs that distinguishes every device, and this can be accessed by an app. The device can also function as a money wallet by enabling payments. Therefore, HI-PGs seem extremely concerned about the combination of these utilities that could be exploited by malicious apps to steal financial information. For example, they said:

> *"I am aware that I have a lot at stake financially and so I must remain safe online especially through my smartphone. Because my phone's unique ID and other information can identify me. Then the fact that I don't feel like my phone is very secure is the reason I try to avoid having sensitive information in my phone."* HI-PG 02.

"…the privacy of my smartphone goes with the security of my bank cards" HI-PG 07. Another respondent said, *"Financial information for example, is much easier to access through your phone because it has* [smartphone] *become a wallet"* HI-PG 04.

The above responses suggest that the economic status of HI-PGs exacerbates their perceived sensitivity to financial information in the smartphone context because of the unique utilities of the device. In other words, perceived information sensitivity of high-income PGs is increased by the smartphone's vulnerabilities (see 7.2.1.1).

As shown in section 6.3.2, perception of information sensitivity is equally high among MI-PGs due to the concern for leakage of financial information. Surprisingly, MI-PGs seems to have higher level of information sensitivity compared to their HI-PG colleagues. This means that MI-PG will need less nudging to protect financial information because they are already sensitised towards information protection. However, this does not imply that they deserve less privacy. The differences in perceived information sensitivity shows the type of privacy support that different user-categories require. Moreover, tailoring privacy implies that user-categories are supported in ways that matches how they perceive information.

Regarding LI-PG responses to the concern for safety of finances, data analysis shows that they perceive financial information as less sensitive due to the stronger influence of rewards compared with HI-PG and MI-PG. The level of sensitivity expressed by LI-PG means that low economic status reduces high privacy concern because the privacy guardian is expected to be extremely concerned about informational privacy.

7.2.2.2 Concern for safety of finances among privacy pragmatist of all income groups (HI-PP, MI-PP and LI-PP)

The analysis of data shows that HI-PP respondents perceive financial information as highly sensitive like the HI-PG. This is because they consider financial information at risk through apps. This was revealed from the participants' responses in section 6.3.1 and table 7.2 summarises their discourse. However, to aid the interpretation, the following example statements are represented below.

> *"most hacking attempt at our personal details is to access people's finances, so this possibility bothers me a lot. I mind what I do with my card details on the device"* HI-PP 13.

> *"my financial transactions are the riskiest information even though I buy things through my smartphone*." HI-PP 14.

The privacy pragmatist is expected to perceive financial information as less sensitive than the privacy guardian. This unexpected trend captures Martin et al. (2016) argument that the current state of privacy research does not capture the full range and richness of the factors that are important to people when they make privacy decisions (See section 3.2.3). This explains the analysis of multiple factors in the current research.

The MI-PP participants' responses to the concern for safety of finances, the data analysis shows they perceive financial information as highly sensitivity. However, their high sensitivity is moderated by information search to mitigate privacy risk. MI-PP engage in information seeking to mitigate risk and obtain privacy-assurance (Beldad et. al, 2011). *"Some apps may be trustworthy, and users are re-assured about their information privacy. This provides comfort to disclose relevant information*" MI-PP 23.

This means that MI-PP can be supported by concise information towards informed privacy decisions. Although MI-PP participants perceive financial information as highly sensitive like MI-PG, they differ in their preferred mechanism for risks mitigation. Whereas MI-PP participants use information seeking, MI-PG are likely to use PET to mitigate privacy risks (see table 7.2). This makes the case for user-tailored privacy support as recommended by Knijnenburg (2017). This will be discussed further in sections 7.3, 7.4 and 7.5.

The LI-PP participants responses towards the concern for safety of finances shows that most LI-PP respondents perceive financial information as less sensitive compared with MI-PG. However, this trend is not surprising because as mentioned in 7.1.1.3, LI-PU participants expressed similar perception towards the concern for identity information.

7.2.2.3 Concern for safety of finances among privacy unconcerned from all income groups (HI-PU, MI-PU and LI-PU)

The data analysis shows that HI-PU like HI-PG and HI-PP participants perceive financial information as highly sensitive due to concerns about the smartphone ecosystem. The way HI-PU perceive financial information is different from how they perceive identity information. This high level of perceived information sensitivity

towards financial information reveals the influence of the high economic status on different types of information.

Regarding the safety of finances, the data analysis shows that MI-PU perceive financial information as less sensitive compared with HI-PU. MI-PU participants' perception is moderated by the convenience of using the smartphone and in turn raises PU trustful attribute (Kumaraguru and Cranor, 2005). For example, *"there are apps you may trust and some that you should not because they just look fraudulent*." MI-PU 34. This suggest that the PU attribute is more influential among the lower economic group. In other words, as economic status decreases, the trusting nature of PU participants seems clearer. This is confirmed when this LI-PU respondent said: *"one cannot refuse disclosure of financial information all the time and be able to purchase* [using the smartphone], *so we must take the risk and expect nothing will go wrong"* LI-PU 45.

Based on the analyses regarding differences in perceived information sensitivity towards financial information, smartphone users are characterised into two more groups. These groups are, (1) users that perceive financial information as highly sensitive and they are the high-income PG, PP and PU, middle-income PG and PP, (2) users that perceive financial information as less sensitive and they are middle-income PU, low-income PG, PP and PU.

Overall, linking the data analysis (chapter 6) with sections 7.1.1 and 7.1.2, it can be concluded that users' economic status influences two main types of concerns among smartphone users. This confirms Milne et al. (2017) assertion that identity and financial information are sensitive information for online users. So far, smartphone users have been characterised into four groups. However, these groups are further discussed broadly as the high and low information sensitivity perception groups.

7.3 Further Discussion of Main Finding Regarding Economic Status

Finding 1a: The critical factor of economic status exacerbates the perception of information sensitivity of high- and middle-income smartphone users in the three privacy categories (PG, PP and PU) regarding identity and financial information. This also applies to low-income PG.

Low economic status has been found as a cause of poor decision making by influencing individuals to trade-off long-term privacy benefits for short-term rewards

(Sheehy-Skeffington and Rea, 2017). However, this research shows that high, middle, and low economic status smartphone users who are privacy guardians, perceive identity and financial information as highly sensitive and as such, are not likely to trade-off privacy for short term rewards.

The literature suggests that economic status influence how users value privacy in different contexts (Acquisti et al., 2013; Carrascal et al., 2013; Sheehy-Skeffington and Rea, 2017). Our findings extend literature by showing how different users value privacy in the smartphone context. We deepen the analysis by accounting for privacy attitude and economic status. Therefore, the research produced more nuanced insight by considering other privacy-influential factors. In doing this, we contribute to methods of analysis in the way dimensional differences across concepts were revealed from income groups and privacy categories (PG, PP and PU). Combining the critical factor of economic status with the privacy categories allowed the nuanced differences in users' sensitivity perception to be revealed through the analysis of multiple factors (Bélanger and Crossler, 2011). The analysis produced the nuances in how and why users' perceived information sensitivity differs. Otherwise, privacy support targeted at smartphone users could assume that all users are the same (Acquisti et al., 2017; Urban and Hoofnagle, 2014). The data analysis confirms that privacy attributes have much influence on users' privacy decisions. For example, regarding the concern for identity information, one low-economic status participant who is a PG said: "*the type of things that I purchase, and the frequency of purchase could reveal my financial worth. I am not comfortable about this*" LI-PG 25 and another low economic status participant who is a PU said: "*I don't think my personal information is worth much to them"* LI-PU 36. This seems to suggest that economic status has a stronger influence if users are less concerned about privacy and a weaker influence if users have high privacy concern. This explains why the critical factor of economic status exacerbates the perception of information sensitivity of high- and middle-income smartphone users in the three privacy categories (PG, PP and PU) including the low-income PG regarding identity and financial information.

Another possible reason for the high sensitivity towards information is the social context of information disclosure. A recent study (Da Veiga and Ophoff, 2020) shows that individuals' information privacy expectation in the UK is very high. High privacy expectation results in high privacy concern when confidence about regulatory

protection is weak (Anic et al., 2019). Our study confirms that UK residents who face similar privacy risks as citizens have high privacy concerns and thus extends Da Veiga and Ophoff (2020) study by showing other factors such as users' economic status responsible for varying privacy concerns across different categories of residents.

Another possible reason for the high perception of information sensitivity among the groups in our analysis is the timing of the empirical study. The empirical study was conducted soon after the General Data Protection Regulation (GDPR) was introduced. The GDPR provides the framework for protecting personal data of EU citizens. Its introduction could have raised the issue of protecting personal information in the minds of individuals. However, all the participants did not perceive information as highly sensitive. Therefore, we argue that economic status and privacy concern categories contributed to the nuances.

Finding 1b: Low-economic status PP and PU perceive identity and financial information as less sensitive, mainly because of perceived benefit and lack of agency.

The earlier finding (1a) reveals the predominant insight regarding economic status, whereas the sub-finding discussed in this section reveals the type of data to which the predominant insight relates including the underlying causes of the finding.

Low-economic status PP and PU perceive identity and financial information as less sensitive compared with high economic status users. However, one low-economic status PP perceive financial information as highly sensitive because of first-hand experience of data breach. Apart from this exception, the influence of economic status and privacy attribute seem to be the same on all low-economic status participants. However, the concern for data breach cuts across other respondents despite not having a first-hand experience of data breach. Only 3 out of the 47 respondents have experienced data breach directly (see subsection 6.1.1). What seems to be the difference as revealed by this respondent (LI-PP 42) is that an experience of data breach could produce a strong impact on perceived information sensitivity. Most data breach in this context happen through malicious apps (Shklovski et al., 2014). As mentioned in Chapter 2 (see section 2.4.1) the prevalence of malicious apps and unauthorised collection of data are factors influencing the perception of information sensitivity by increasing the risk of disclosure (Kulyk et al., 2019). Increased risks will result in cautious decisions such as withholding or fabrication of information.

Another important aspect of this sub-finding is that it extends the literature on immediate gratification. Immediate gratification refers to the tendency to value present benefits more than future risks (Kokolakis, 2015). However, the category of users that prefers immediate gratification and the types of information that users would giveaway for immediate gratification is unclear. As Kokolakis (2015, p.1) said: "we call for synthetic studies […] that take into account the diversity of personal information and the diversity of privacy concerns". Therefore, our findings show that low-economic status PP and PU are more likely to be influenced by immediate gratification regarding identity and financial information than other categories of users.

Linking this finding which is enabled by Westin's characterisation with Hann et al., (2007) ranking of online users, we can conclude that low-economic PP and PU are convenience seekers, who are willing to exchange information for convenience (Hann et al., 2007). However, the danger here is the justifying of unwarranted collection of such users' personal information by offering conveniences. Doing this will neglect the worrisome aspects of personal information collection. However, our analysis shows that low-economic PP and PU participants expressed some level of perceived sensitivity which should not be neglected. Therefore, this finding has implication for how organisation's privacy policy is designed. As discussed in chapter two, specifically section 2.3, privacy is a fundamental human right protected by regulations, for example, the GDPR. However, the burden of understanding when, what and with who to share personal information or raising complaints if privacy right is violated rest on individuals. This burden can be reduced through meaningful support. To achieve this, Martin et al. (2016) argues that understanding how different categories perceive privacy concern should be considered. This helps organisations respond with right policies, products, and services. Moreover, perception of information sensitivity shows users desire to mitigate privacy risks in order to function effectively in digital environments (Kim and Koohikamali, 2015; Markos et al., 2017; Noain-Sánchez, 2016). This implies that all the different levels of information sensitivity are saying something about users' desire for privacy protection. Table 7.3 below summarises the main findings and contributions about economic status.

Table 7.3: Summary of main findings and contributions to literature from this section

Literature	Finding	Contribution	Implication
Low economic status results in undervaluing privacy by trading off long term consequences for short term rewards (Sheehy-Skeffington and Rea, 2017).	Low-economic status PGs are not likely to trade off privacy for short term rewards.	Applying economic status directly to privacy decisions in the smartphone context. Economic status has a stronger influence if users are less concerned about privacy and a weaker influence if users have high privacy concern.	Economic-status is a critical factor that can reveal how distinct categories of users (PG, PP and PU) can be supported towards user-tailored privacy.
Immediate gratification is the tendency to value present benefits more than future risks (Acquisti and Grossklags, 2005; Kokolakis, 2015).	low-economic status PP and PU are more likely to be influenced by immediate gratification regarding identity and financial information than other categories of users.	Segmenting the generalised assumption regarding how immediate gratification applies. E.g., LI-PP and PU affected by immediate gratification. Conversely, HI-PG, PP, PU and MI-PG, PP are less likely to be affected	Draws attention to the most vulnerable users that require institutional protection with proper policies, products, and services.

7.4 The Influence of Location Tracking

This section interprets the categories that emerged from the perspectives of the three privacy categories (PG, PP and PU) regarding the influence of location tracking on how users perceive information. The emerged categories are the varying personal, situational, and profiling concerns regarding location tracking. Personal concerns relate to users' perception of vulnerability about location tracking. However, this perception is moderated by the convenience of using the smartphone among PP and PU. Situational concerns relate to how users judge the appropriateness of location

tracking and profiling concerns relate to the inference that could be made from location tracking to other areas of privacy through implicit data.

How the core category functions are illustrated in Figure 7.1 below. The topmost node represents the different categories that emerged from data analysis in chapter six. The categories explain different phenomena across the various groups (PG, PP and PU) as the second row of rectangular nodes indicates. The direction of arrows shows direct line of influence. For example, the arrows pointing from personal factors category (PP and PU) through convenience and benefits to location tracking indicates that PP and PU participants are influenced by the convenience and benefits of using the smartphone. The bottom set of rectangular nodes indicates how privacy concern regarding location tracking influences PG and PP/PU perception of information sensitivity.

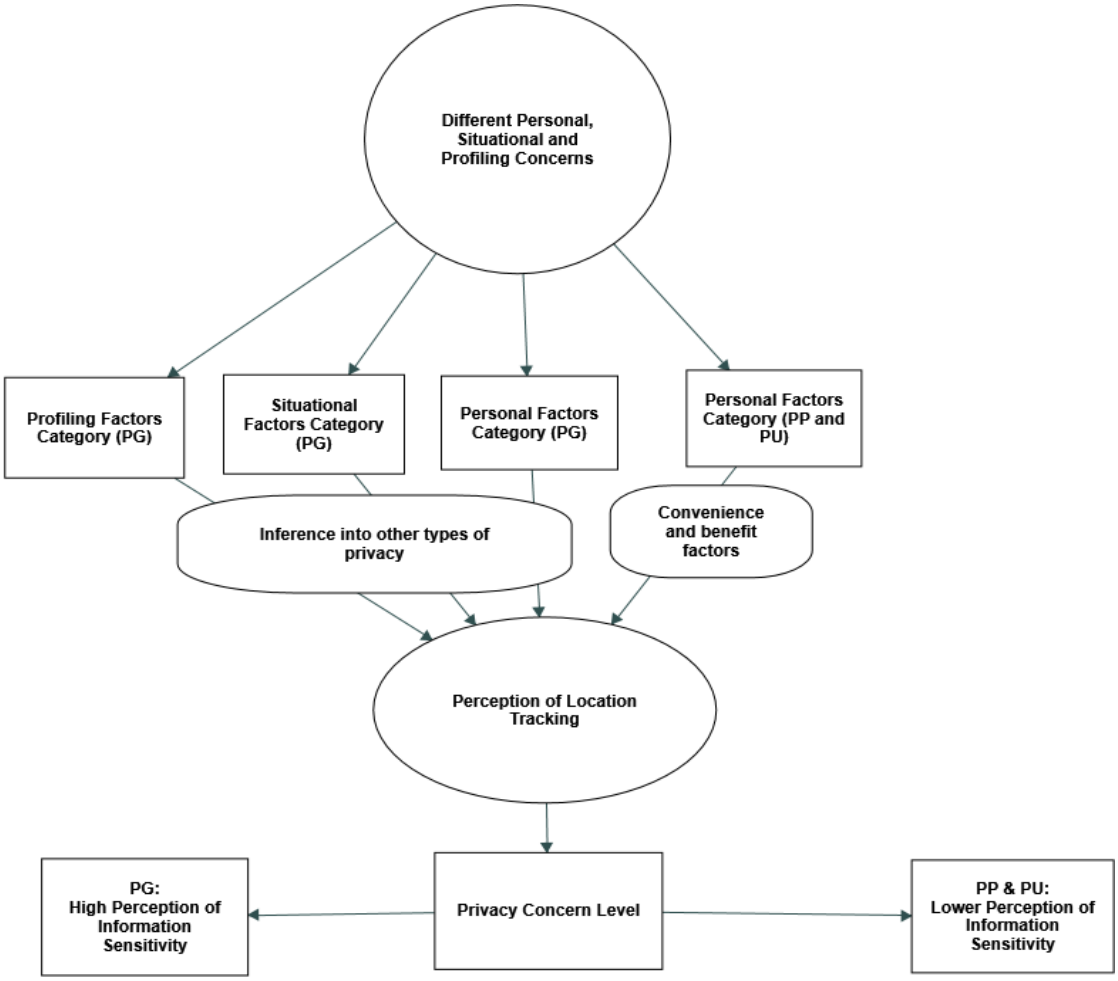

Figure 7.1: Illustrates how the categories provide different insights regarding distinct users.

Regarding PGs, the data analysis shows that location tracking has a strong influence on how participants perceive location information. Although there are several reasons for the high sensitivity perception, the majority fall under one basic cause. These reasons are captured as the strong concern about inferring other aspects of privacy from location information. In other words, location information is a source of implicit data. Implicit data refers to inferred data (Dobson and Fisher, 2003; Guinchard, 2020). According to this respondent, *"Location tracking is a huge concern because from there you can track secondary information about the person*" PG 07. This came out more explicitly when another respondent said:

> *"…if you go to the same place every day, they can know that's the place you work or where your home is or where your friends are, even where your kids go to school without ever sharing that information*." PG 01.

This suggests that the critical nature of an influencing factor like location tracking can shape privacy concern and the corresponding information sensitivity perception. Moreover, the literature points out that PGs typically show high concern for their personal information (Kumaraguru and Cranor, 2005). However, this does not explain whether other factors can either heighten or lessen this concern. Therefore, our analysis suggests that the interaction between the PG's high privacy concern and the critical nature of location tracking in the smartphone context seems to explain why PGs perceive location information as highly sensitive. High perceived sensitivity confirms the implicit information that location tracking provides. For example:

> *"When your camera app request for your location* [location information], *they want to add that information to your photo, when you share the photo, you share the information about where that photo was taken, so I denied the app access to my location"* PG 04

This response and other similar ones confirm the criticality of location tracking. The fact that the smartphone is carried about by users strengthens the criticality of location tracking and show why this factor exacerbates PG users' sensitivity perception. This explains why PGs see location tracking as a form of digital surveillance (Amit et al., 2020; Kokkoris and Kamleitner, 2020) and thus they feel

vulnerable; *"Just imagine there is a virtual person following you everywhere you go" […] "This is really a frightening prospect*" PG23.

Since most PGs expressed higher perception of sensitivity towards location tracking, they are less likely to disclose location information. However, a few PGs expressed less sensitivity towards location information by emphasising the benefits attached to disclosure: *"…there have been instances where I needed a map to show me location or proximity so then I had to share my location*" PG 23. However, benefits and convenience weighs little in terms of influencing how PGs perceive location information. Therefore, we can induce that location tracking make PGs perceive location information as highly sensitive except in a few cases.

Regarding the influence of location tracking among PP and PU participants, several reasons were found in the data analysis as influencers of perceived information sensitivity (see 6.3.4). However, the majority fall within the convenience and benefits derived from using the smartphone (see figure 7.1). When compared to PGs, PP and PU participants perceive information as less sensitive because they are more benefits-inclined than risk averse. Examples of responses regarding perceived sensitivity are:

"I will usually disable the location permission after downloading the app and enable it when I need to use the app for navigation, to avoid apps capturing all my journeys" PP08.

"this [location] tracking makes me feel exposed everywhere" PP10. Other examples regarding convenience and benefits are**:**

"the convenience and benefits of using fitness and mapping apps makes up for the creepiness of tracking me since I don't have anything to hide" PP 29

"I need the app to provide direction for me" PP15

"It is really convenient to use apps like Waze and Google maps for direction" PU 17.

"location tracking can be beneficial as it can be an alibi [digital evidence of location] to prove one's innocence when it matters. Having a history of my movement has obvious benefits" PU 32

The above statements and many others suggest that most PP and PU respondents have higher consideration for convenience and benefits surrounding the use of the smartphone, hence they have lower sensitivity. This means that PU are not unconcerned about personal information as the Westins privacy index suggests (Kumaraguru and Cranor, 2005). However, our analysis confirms the literature that

PU concern is low compared to other groups when other factors (e.g., high economic status) are not considered. Their level of concern and sensitivity depend on the type of information, benefit, or conveniences at stake. Highlighting the areas of PP and PU participants' sensitivity is important otherwise the worrisome aspects could be neglected.

Based on our findings regarding differences in perceived information sensitivity towards location tracking, we characterise smartphone users into two additional groups. These groups are, (1) users that perceive location information as highly sensitive and they are the privacy guardians and (2) users that perceive location information as less sensitive and they are the privacy pragmatists and privacy unconcerned. The next section discusses the main finding from the data analysis regarding PG, PP and PU.

7.4.1 Further Discussion of the Findings Regarding Location Tracking

Finding 2: The critical factor of location tracking heightens the perception of information sensitivity among PG users because of personal, situational, and profiling concerns. Conversely, PP and PU users perceive information as less sensitive due to a higher influence of personal concerns.

As Illustrated in figure 7.3, location tracking expose users to privacy risks that influences how information is perceived. However, sensitivity perception varies by user's privacy concern category which in turn is affected by bounded rationality. Consequently, a user's privacy decision will be strongly influenced by their perception of information sensitivity, resulting in either restricting or allowing access to location information.

Location tracking have been found as a concern for smartphone users in earlier studies (Almuhimedi et al., 2015; Amit et al., 2020; Kokkoris and Kamleitner, 2020). Hence Ghazinour et al. (2014) argues that supporting individuals' location privacy is critical. Doing this requires an understanding of how location tracking influences different categories of users (Kokkoris and Kamleitner, 2020). Our finding makes this contribution.

Our finding confirms the literature that location tracking triggers privacy concern because of surveillance issues (Almuhimedi et al., 2015; Amit et al., 2020; Kokkoris and Kamleitner, 2020). What differentiates our finding from earlier literature is that it

provides nuances on how different categories of users perceive information and lays the foundation for a more accurate privacy support. Accurate privacy support requires the understanding of varying levels of perceived information sensitivity. In providing this insight, we show that PGs perceive location information as highly sensitive because of the critical nature of location tracking in this context. Most PG participants point out location tracking as a profiling concern factors. This is because a user's social life can be inferred from location tracking. For example, "*Sharing my location information is not a thing I really like to do because, tracking my location continuously can give me away as a frequent visitor of a specific pub…."* PG 24. This type of reason can be distinguished from the types expressed by most PP and PU. The analysis shows that PP and PU perceptions are influenced by the conveniences and benefits associated with smartphone use. Whilst not offering an exhaustive list of information sensitivity influencers, participants across the privacy categories pointed to the personal, situational, and profiling concerns (see details in table 6.7). These concerns are influencers of users' perception of information sensitivity.

The high perception of information sensitivity among PGs is not surprising. Westin's privacy characterisation (Kumaraguru and Cranor, 2005) and Hann et al. (2007) privacy ranking had indicated that PGs are highly concerned about personal information. However, our finding extends the information privacy literature in another area. Specifically, the study by Bansal et al. (2016) who argue that information sensitivity is situation-specific but did not say which situation. Therefore, we found situations such as the proper use-case for navigation that reduces perceived information sensitivity of location tracking. For instance, one PG mentioned that: *"I will give my location data if, for example, I am using GPS app for navigation. Afterwards, I will disable it."* PG 40. This shows a situation that shapes perceived information sensitivity. Therefore, specific situations should be accounted for when analysing perceptions of information sensitivity.

Privacy pragmatists and privacy unconcerned users' low sensitivity perception regarding access to their location information have been attributed to the greater effect of convenience and benefits. In addition, a lack of agency based on the realisation that most apps collect location information without users' consent as mentioned in chapter 2 explains this perception. This interpretation agrees with Acquisti (2004a, p. 3)"…*that sophisticated privacy advocates might realise that protecting themselves*

from any possible privacy intrusion is unrealistic". Therefore, they may not adopt a strict privacy protection strategy since they doubt it will eventually pay-off. Therefore, short term benefits may be preferred as this PP participant said: "…*the convenience and benefits of using fitness and mapping apps makes up for the creepiness of tracking me since I don't have anything to hide*" PP 29. However, the long-term effect of not protecting such privacy-critical information could be costly, leading to potential losses in the smartphone context.

In concluding this section, prior research (Bansal et al., 2016; Markos et al., 2017; Milne et al., 2017) argues that information sensitivity predicts information disclosure (see Chapter 3). However, information sensitivity will be more predictive and thus valuable if it distinguishes the varying impact of privacy influencing factors. For example, location tracking and its situational influencers as our finding shows. Awareness of such nuances should be incorporated in theoretical and empirical works on privacy, as well as into privacy policy making. Table 7.4 provides the summary of main findings and contributions regarding location tracking.

Table 7.4: Summary of main findings and contributions regarding location tracking

Literature	**Finding**	**Contribution**	**Implication**
Location tracking is a concern for smartphone users in earlier studies (Almuhimedi et al., 2015; Amit et al., 2020; Kokkoris and Kamleitner, 2020).	Location tracking heightens the perception of information sensitivity among PG users Conversely, PP and PU users have lower perception of information	Nuanced understanding of the varying influence of location tracking in the smartphone context.	Supports user-tailored privacy protection.
Information sensitivity is situation-specific but did not say which situations (Bansal et al., 2016)	Finds specific situations influencing information sensitivity regarding location tracking	Highlighting some specific situations that should be accounted for when analysing perceptions of information sensitivity.	Supplies the nuanced differentiation and the reasons for the distinct levels of perceived sensitivity across the categories of users

	E.g., proper use-case for navigation can reduce perceived sensitivity of location tracking		and thus lays the foundation for a more exact privacy support
The value of information sensitivity is the predictability of information disclosure (Bansal et al., 2016; Markos et al., 2017; Milne et al., 2017)	We found that location tracking contributes to information sensitivity in varying ways based on users' privacy concern category.	Enhanced value of information sensitivity by distinguishing the varying impact of location tracking	Such nuances should be incorporated in theoretical and empirical works on privacy, as well as informing privacy policy making

7.5 The Influence of App Permission Request

The earlier section raised the issues regarding location tracking. This section interprets the categories that emerged from the perspectives of the three privacy categories (PG, PP and PU) regarding app permission request. The interpretations draw from the data analysis in section 6.3.5. The categories that emerged are *privacy concerns and perception of control*. These are influencers of varying sensitivity perceptions to app permission request. How the core category functions is illustrated in figure 7.2 below. The topmost rectangular node indicates the influencing factor. The next node (circular) indicates the combined effect of the categories. Next, the two rectangular nodes pointing (using arrows) through consequences of wrong disclosure and perceived control nodes indicates that concern and control perceptions operate differently across PG, PP and PU. The bottom row of nodes shows the different levels of information sensitivity.

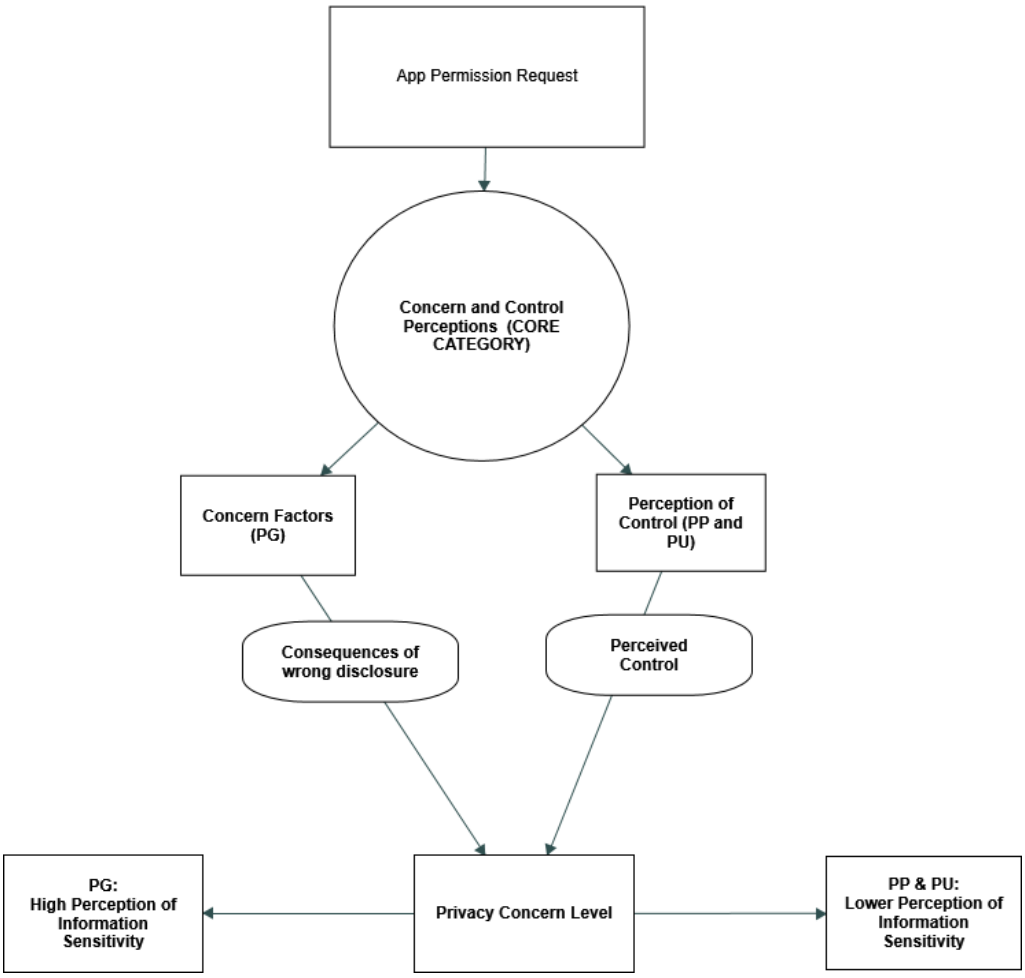

Figure 7.2: Illustrates the core category and varying influence of App permission request.

Regarding PGs, the categories in figure 7.2 shows that PGs perceive information as highly sensitive because they are more mindful of the consequences of wrong disclosure. So, they want to make autonomous disclosure without disguised interference (see table 6.9). They are particularly distrustful of apps that make unjustified request and will avoid those types of apps. Explaining the high sensitivity, some respondents said:

"*those requests call me to make a huge decision that can have profound consequences if it goes wrong"* PG 26.

"*What is most important to me is keeping my autonomy and making sure that the decision I make whether I want to share something or not is right". PG25*

"my autonomy is also about making sure that it's my decision to share what I want to share and not to be unduly influenced through quick nudges. This is particularly important" PG 27

Some participants are using the word autonomy to mean privacy because as Alfino (2001, p. 7) argues "…privacy protects a "fundamental interest" one has in "being able to lead a rational, autonomous life (see section 4.4.2).

Unjustified request plays a role in raising how PGs perceive information. This is exemplified by the following statements: *"I think it's the task of the developers and providers to explain why they need certain data"* PG 37. So that PGs can be assured because*: "that will make the user have a much better feeling for what they are actually sharing"* PG 41. In addition, another respondent said: *"At the moment, most providers are of the view that the more we collect, the better. So, let us just collect as much as possible*" PG 38. Linking the findings in section 6.3.5 to that of this section, it can be concluded that app permission requests heighten PGs perception of information sensitivity because of the prevalence of malicious and unjustified requests. As discussed in detail in section 7.7 below, PG's desire to limit access to their personal information could be a factor to this finding.

PP and PU participants show similarities in perceiving app permissions with less sensitivity. Most PPs and PUs perceive app permission request with less sensitivity because they perceive app permission as a form of control over personal information. However, they require short justification of each request. Explaining why they perceive app permission with less sensitivity, this respondent said: "…*because that gives me the choice to say no. Some apps now have runtime requests that ask for access when you need to use certain services*" PP 31. Another participant added, *"But I appreciate they [apps] ask and not doing it* [accessing user information] *without asking me…" PU 36.* Furthermore, they provided explanation for the perception of control: *"I am quite happy when I see the request…"* PP29. *"…. So, that choice is something that gives me a sense of control." PP 31.*

Unlike PP, some PU participants perceive certain types of information as highly sensitivity, "*…However, when apps want to access my contact, that's going to be a problem. I don't want somebody having a list of my contacts."* PU 36. The creation of privacy zones could be a factor to these types of responses because people

create “privacy zone” as instrument of control over information that should remain private or over how much of it should be shared.

Linking the findings in section 6.5.5 and table 6.9 to the interpretations in this section, it can be concluded that app permission request triggers low perception of information sensitivity among PP and PU users by influencing the perception of control over access to personal information except over contact list and photos. The respondents that expressed these exceptions are women. This suggests that a respondent’s gender could influence the creation of varying privacy zones.

On the basis of our findings regarding app permission request, we characterise smartphone users into additional two groups. They are, (1) users whose perceived information sensitivity is heightened by app permission requests - privacy guardians and (2) users who perceive apps permission request as a source of control over information requests thus perceiving app permission request with less sensitivity and they are the privacy pragmatists and privacy unconcerned. The next section further discusses the main finding.

7.5.1 Further Discussion of the Findings Regarding App Permission Request

Privacy guardians (PG) perceive app permission requests with high information sensitivity because they are concerned about malicious and unjustified requests. Conversely, privacy pragmatist (PP) and privacy unconcerned (PU) users perceive it with less sensitivity as it gives them a false perception of control over their personal information except over contact list and photos.

Earlier studies (Bansal et al., 2010a; Milne et al., 2017; Schwartz and Solove, 2011) point out that information sensitivity varies by types of personal information. However, this research extends the literature by showing that perception of information sensitivity regarding app permission request varies by categories of smartphone users and in some cases by types of personal information.

As seen in Figure 7.2, data analysis shows that apps permission request expose users to privacy risks. Consequently, a user’s privacy decision will be strongly influenced by their risk perception and the value of the information that is requested by an app. This explains why PG users are more sensitive to personal information than PP and PU because PGs typically have high privacy risk perception. However, the value users attach to information is sometimes influenced by demographic characteristics such as

gender (see sub-section 6.6.2). Apps behaviour for requesting access to sensitive information contributes to users' information sensitivity.

A recent study (Furini et al., 2020) shows the typical types of app request that users are sensitive to. They include requests for location data, personal contacts, and photos. However, why users' perceived information sensitivity to app requests differs is unclear. Therefore, we extend this literature by providing further explanation why and how smartphone users' information sensitivity level differs by linking privacy attributes and contextual factors. Furthermore, the connection between context and information sensitivity is not new. Some researchers (Bansal et al., 2016; Milne et al., 2017; Mothersbaugh et al., 2012) have argued that information sensitivity is contextual. Therefore, our finding confirms this literature in the smartphone context and extends it by showing the type of users with varying levels of information sensitivity. For example, PGs believes that they have lost too much privacy already, therefore, they are uncomfortable with the decision-making burden under the uncertainties imposed by apps permission request. They said: *"…those requests call me to make a huge decision that can have profound consequences if it goes wrong"* PG26. Whereas most PPs are: *"… quite happy when [they] see the request…" PP 29.*

> *This is "…because that gives [them] the choice to say no, as some apps now have runtime requests that ask for access when you need to use certain services. So, that choice is something that gives me a sense of control."* PP 31

Similarly, PU "… *appreciate* [the permissions]. However, when the apps want to access […] *contact list, that's going to be a problem… because an app has stolen my contacts before..."* PU 36. However, the phrase "…*when the apps want to access […] contact list, that's going to be a problem…"* seems to suggest that PUs perceive contact information as more sensitive. When this statement was compared with other PUs, it was discovered that such exceptions are because of negative experience of data breach. This was "…*because an app has stolen my contacts before*" PU36. This suggests that experiences of data breach influences how each privacy category perceive information and thus explains the few outliers. However, this does not mean that users' perception cannot be characterised according to privacy concern categories. Generally, PU participants are willing to exchange information for convenience. This attitude can be attributed to lack of knowledge about privacy risks as confirmed by Furini et al. (2020). This also explains why several PU participants

expressed lack of agency. A counter measure is better risk communication as studies (Gates et al., 2014; Hatamian et al., 2019; Van Wassenhove et al., 2012) have found that better risk communication results in better risk mitigation.

Studies have shown that advertised and implemented app behaviour do not match (Alazab et al., 2020; Olukoya et al., 2020). This suggests that malicious apps make disguised request to access users' resources. The knowledge of these practices exacerbates privacy concern. Our analysis found that PGs are more sensitive to these practices. Therefore, enhancing permission requests through better textual or symbolic description can reduce the perceived sensitivity of PGs towards app permissions (Olukoya et al., 2020). Therefore, developing tailored-permission requests that provides privacy assurances to different categories as Knijnenburg, (2017) advocates could be a counter measure. Our study deepens the privacy perception study by contributing the basis for applying nuanced app permission requests. We advance the conversation from a general app request model to a more segmented, users-tailored model that should support every user's privacy (see subsection 7.2.1.3).

In conclusion to this section, we argue that because "no one method fits all", a user-tailored app model is important. Moreover Martin et al. (2016) argues that understanding how different categories of people perceive privacy concern will lead to developing the right privacy policies, products, and services. Highlighting the nuanced sensitivity perceptions reveal users' specific expectations for privacy assured disclosures which informs the development of a user-tailored- app permission requests (Pavlou, 2011; Xu et al., 2011a). Table 7.5 below summarises this discussion.

Table 7.5: summary of findings and contribution regarding apps permission request

Literature	Finding	Contribution	Implication
Perception of information sensitivity influence user responses and are contextually driven. (Bansal et al., 2016; Milne et al., 2017; Mothersbaugh et al., 2012)	Apps behaviour for requesting access to sensitive information contributes to users' high perception.	Applied perception of information sensitivity to understand the influence app permission request on distinct categories of users	Tailored-app permission requests
Advertised and imple mented app behaviour does not match (Alazab et al., 2020; Olukoya et al., 2020).	PG Users are suspicious of permission requests. PP and PU users, feels it gives control over personal information	Specific understanding of how user groups vary in responses	Advances the conversation from a general app request model to a more segmented, users-tailored app permission request model
Publicity rule creates awareness of risk and benefits of disclosure leading to creation of privacy zones (Tavani, 2008)	Insights on users' perception of information sensitivity to inform the creation of privacy zones around more sensitive information	Proposition for using differences in perceived information sensitivity towards APR to improve users' privacy	Privacy zone help users discriminate disclosures

7. 6 The Influence of Bounded Rationality and RALC Theories on the Perception of Information Sensitivity

This section aims to better understand the perception of information sensitivity through the lenses of the theoretical framework. In addition, Grounded Theory is typically about seeking deeper explanation of phenomenon and models can be useful tools (Braun and Clarke, 2013). The model presented below (figure 7.3) is the result of the study which seeks to understand how critical factors influence smartphone users' perception of information sensitivity based on their privacy concern categories. Doing

this provides the insight on how and why different users respond to privacy risks, to enable nuanced privacy decisions support.

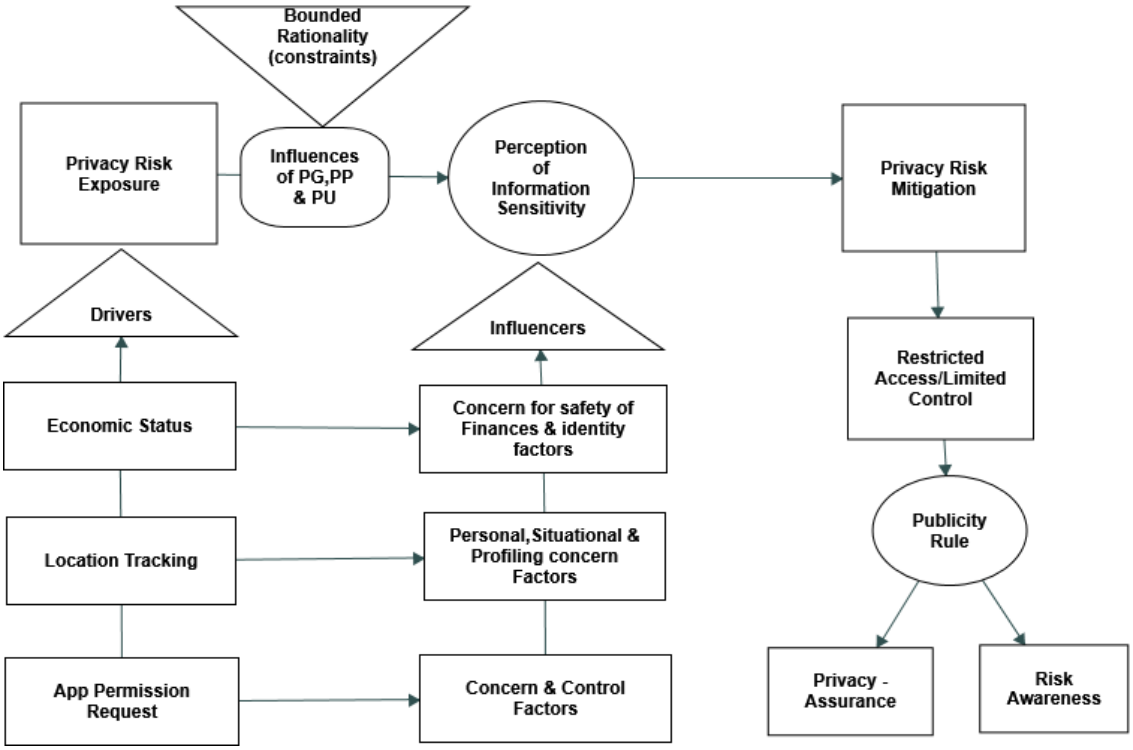

Figure 7.3 Integrated theoretical framework and research findings

The constructs of the model are drawn from the literature review and the empirical data analysis. This helps to provide theoretical explanation of the findings towards developing a middle range theory. Middle range theories are testable propositions about the phenomenon investigated. Regarding the drivers of privacy risk in the model, other research have found location tracking (Almuhimedi et al., 2015; Guinchard, 2020; Kokkoris and Kamleitner, 2020), economic status (Huberman et al., 2005; Sheehy-Skeffington and Rea, 2017) and app permission request (Taylor and Martinovic, 2016; Wang et al., 2017) as influencers of privacy decisions. However, our research justified the criticality of these factors in the smartphone context (see chapter 2). Strauss (1998) recommends theoretical integration and validation as the last stages of GT (see section 5.9 and figure 5.2). So, the bounded rationality and restricted access and limited control (RALC) theories as revealed in Chapter 4, will be discussed in terms of how the theories explains the findings or how the findings depart from its constructs, thus seeking to advance theory. As our analysis found, bounded

rationality shapes information sensitivity and RALC provides mechanisms for countermeasure. The connection between the two theories as figure 7.3 illustrates is that one side represents privacy decision making challenges (bounds of rationality), and the other side (RALC) represents countermeasures.

Given earlier discussions (see sections 7.3, 7.4, and 7.5) the model drawn from the empirical findings confirms that the critical factors drive privacy risk. For example, economic status increases or decreases the value users place on personal information. This value shapes privacy concerns which in turn influence how information is perceived. Furthermore, our analysis shows that users' perception of information sensitivity is affected jointly by users' privacy concern category (PG, PP and PU) and bounded rationality as illustrated in the integrated model (figure 7.3). Bounded rationality imposes bounds or challenges on user's ability to make optimal privacy decisions. The bounds on rationality exacerbate or lessen sensitivity perception based on a user's privacy concern category. Sensitivity perception decides privacy mitigation, resulting in restricting access to personal information. The RALC provides mitigation in form of the publicity rule mechanism. Understanding varying sensitivity levels underpins how privacy support is appropriately applied to users through risk awareness and privacy assurance information. This has been explained in sub-sections 7.2.1.3 and 7.6.1.

The principal theme connecting the main findings relating to the factors of economic status, location tracking and app permission request (see sections 7.3, 7.4, and 7.5) shows that perception of information sensitivity is highest among privacy guardians and lower among privacy pragmatist and privacy unconcerned users except in few cases (see section 6.2.3.1). These exceptions depend on users' income status and the type of information involved. For example, the findings regarding the factor of economic status shows that the perception of information sensitivity is highest among the high- and middle-income smartphone users across the three privacy categories (PG, PP and PU) regarding identity and financial information. However, when it comes to the low-income users, only PGs have high sensitivity towards identity and financial information. Conversely, low-economic status PP and PU users perceive information as less sensitive. This means that there are differences in perceived sensitivity based on both income and privacy concern categories. Although earlier literature (Hann et al., 2007; Kumaraguru and Cranor, 2005) have characterised people into three

categories based on their levels of privacy concern, our findings show that smartphone users can be characterised into eight groups based on differences in perceived information sensitivity to the critical factors investigated. These groups have been pointed out under the discussion of each critical factor (see sections 7.2.1.3, 7.2.2.3, 7.4 and 7.5).

7.6.1 Understanding user sensitivity perceptions through bounded rationality and RALC

The relevant components of the concept of bounded rationality are shown in chapter 4. These are, (1) Incomplete information, (2) time constraints, and (3) cognitive limitation. These components help to understand the high perception of information sensitivity among smartphone users. For example, when PGs with high level of privacy concern do not have full understanding of the disclosure and do not have enough time and cognitive ability to process and understand how information is used, uncertainties are created. Uncertainties about how personal information will be handled results in perceiving information as highly sensitive (Kim and Koohikamali, 2015; Mothersbaugh et al., 2012). However, similar uncertainty due to incomplete information about the risks involved in disclosing personal information explain why PU users perceive information as less sensitive. This is because when they do not perceive disclosure risks due to incomplete information, they make unwarranted disclosure (Kumaraguru and Cranor, 2005). Studies shows that when effective risk communication takes place, individuals such as PUs adopt better risk mitigation. Therefore, Acquisti et al. (2017) recommends nudging individuals towards informed disclosure. Our findings extend the study by Acquisti (2017) by showing how users can be nudged differently by understanding their levels of information sensitivity. Smartphone users with high sensitivity perceptions such as privacy guardians and other high-economic status users as well as low sensitivity users should be supported with relevant risk communication (subsection 7.2.1.3) to avoid unwarranted disclosures. Furthermore, users' levels of information sensitivity can be linked to users' responses; information seeking, withholding of information, and fabrication of information (see section 3.5).

Users with high perception of information sensitivity (PGs) are more likely to mitigate privacy risk through information seeking (see section 6.2.1.3). However, they could withhold or fabricate information when unable to verify the need for disclosure (see

section 6.2.2.1). For example, being able to make independent judgement whether to disclose is important: They said: *"my autonomy is also about making sure that it's my decision to share what I want to share and not to be unduly influenced through quick nudges. This is particularly important"* PG 27. Therefore, data collectors should nudge users by applying the choice and consent part of RALC. Doing this aligns data collection to users' preferences. This creates an equilibrium in interest between users and data collectors. This is important because Individuals can receive help from personalisation of products and services, whereas collectors can boost their ability to address specific target markets or customers (Acquisti et al., 2016; Anderson et al., 2017). Therefore, users should be nudged differently to ensure privacy for the different levels of information sensitivity. This has been explained in section 7.6, 7.2.1.1 and 7.5.1. In this regard, the "publicity rule" emphasised by RALC captures the use of nudges which addresses some of the constraints imposed by bounded rationality. The publicity rule creates awareness of risk and benefits of disclosure (Tavani, 2008). However, our data analysis suggests that the publicity rule should be more applicable by tailoring towards the sensitivity perceptions of different users. In this way, the awareness of risks can empower users to create diverse types of privacy zones. This explains why some users for example, perceive financial information as more sensitive than other types of information as shown by the privacy zone created around financial information (see section 7.3.1). Our data analysis extends the RALC theory by suggesting ways of making it more applicable to this context (figure 7.3 illustrates this extension).

7.7 The Middle-Range Theory for Understanding Smartphone Users' Perception of Information Sensitivity

As stated in chapter one, the overall aim of this research is to understand smartphone users' perception of information sensitivity from three privacy concern categories. Doing this provides insight for tailored privacy. Tailored privacy supports users differently by using relevant risk communication. Propositions showing the differences in perceived information sensitivity provides this understanding. Having theoretically examined the principal finding of the research, this section articulates the resulting middle range theory that emerged from the data analysis. As mentioned in Chapter 4 (section 4.2) middle range theories stem from more nuanced analysis of individuals' attributes which differs from analysing the interactions between individuals. To achieve this, this researcher applied Hassan and Lowry (2015) and Hassan et al.

(2019) framework for developing middle range theory. Table 7.6 below presents the summary of the framework guiding the formulation of the theory.

Table 7.6: Summarises Hassan and Lowry, (2015) and Hassan et al., (2019) guidelines and the application

Hassan and Lowry, (2015) and Hassan et al., (2019) Framework Guideline	**How it is Applied**
A focus on solving a problem or addressing a question within a limited domain	A focus on formulating effective privacy-support for smartphone users. Thus, investigated 3 critical and contextualised factors influencing information sensitivity in smartphone use.
Create intermediate concepts and propositions that operate between grand theories and minor working hypotheses	Developed middle range theory as testable propositions for understanding varying levels of information sensitivity across user-categories
Develop and refine the concepts and propositions by focusing on the specific phenomena	Developed GT analysis concepts (open, axial, and selective coding) focusing on extracting users' perception of information sensitivity inferred from the discomforts and concerns expressed.
Evaluate the originality and novelty of the propositions by comparing with the literature.	**Studies on information sensitivity in the general online context**: Bansal et al., (2010), Mothersbaugh (2012), Capistrano and Chen (2015), Markos et al., (2017), Mekovec et al., (2017). **Studies that show smartphone users differs by other constructs apart from information sensitivity.** Application usage and demography: Zhao et al., (2016) Okamoto et al., (2017), Welke et al., (2016) Falaki et al. (2010), Dinev (2014), Bhih et al., (2016), Mohadisdudis and Ali, (2014) and Security perception towards notifications: Ndibwile et al., (2018). **Studies that focused on user's perception of information sensitivity in smartphone context**: App permission request Furini et al., (2019). However, we investigated app permission request, economic status, location tracking. Thus, our propositions differ by accounting for the three critical factors.

The following propositions aim to answer the third research question which is:

How do the identified critical factors influence the perception of information sensitivity among smartphone users based on their characterised privacy concern?

Proposition 1: Smartphone users' privacy concern category and economic status influence how they perceive types of information.

Proposition 2: Users belonging to all three privacy concern categories with high-and-middle economic-status perceive financial information as highly sensitive. The exception is the middle economic-status privacy unconcerned.

Propositions 3: Users that perceive financial information as less sensitive are middle-income privacy unconcerned and low-income users from the three privacy categories.

Propositions 4: Privacy guardians of all economic status and privacy pragmatist of high economic status perceive identity information as highly sensitive.

Propositions 5: Privacy pragmatists and privacy unconcerned of high, middle, and low economic status perceive identity information as less sensitive.

Proposition 6: Location tracking makes privacy guardians perceive location information as highly sensitive, except when location tracking is considered appropriate.

Proposition 7: Privacy pragmatist and privacy unconcerned users perceive location information as less sensitive due to the benefits of using the smartphone.

Proposition 8: App permission requests triggers higher information sensitivity perception among privacy guardians compared to privacy pragmatist and privacy unconcerned users when the request is perceived unjustified.

Proposition 9: Apps permission requests influences a false perception of control among privacy pragmatists and privacy unconcerned users and in turn produces a weaker effect of information sensitivity.

The propositions relating to economic status, location tracking and app permission request from the three privacy concern categories shows that smartphone users can be characterised into eight categories based on how and why users perceive different types of information. The above propositions suggest that an effective privacy support

model for smartphone users should consider the nuances underpinning perceived information sensitivity.

7.8 Conclusion

The interpretation and discussion of findings in this chapter build on the empirical data analysis in chapter 6 and review of existing literature in Chapters 2 and 3, as well as the theoretical framework in chapter 4. The findings were structured under three broad categories, namely: (1) the influences of economic status from the three-income status and privacy categories, (2) the influence of location tracking from the three privacy categories, and (3) the influence of apps permission request from the three privacy categories. The privacy categories are privacy guardians (PG), privacy pragmatist (PP) and the privacy unconcerned (PU).

The discussion in this chapter explains how users perceive information as either highly or less sensitive by pointing out the influences of the critical factors within the smartphone context. Other studies have focused on explaining individuals' motivation to protect personal information from unauthorised access and collection. The current study focuses on group level analysis, thus exploring the complexities between privacy attributes and privacy-critical factors in the smartphone context. Applying this analytical approach enabled the contribution of nuanced understanding regarding how the perception of information sensitivity differs across the eight characterised categories. Doing this points out how to accurately provide privacy support for different groups of smartphone users. When data collectors take the varying sensitivity perceptions into account, privacy in the smartphone context should be enhanced.

Finally, the chapter examined the influences of the concept of bounded rationality and RALC theory on users' perception of information sensitivity and uses insight from the empirical findings to develop the testable propositions. The next and concluding chapter presents the overall summary of the grounded theory research study, research contributions, limitations of the study, recommendations for future research.

Chapter Eight

8. Research Conclusion and Future Research

The aim of this research is to understand the differences in perceived information sensitivity among smartphone users. This is important because it shows the nuances required for implementing tailored privacy. Tailored privacy supports individuals by using the information that will enhance privacy.

Information sensitivity is an influencer and predictor of privacy decisions. However, privacy decision making is complex to understand due to its context-dependency and multi-factor influences. Without accurate understanding of the contextual influences, providing the required support for smartphone users will be problematic. This makes the understanding of how user-categories perceive information useful for tailored-privacy support. To enhance user privacy in the smartphone context, data collectors should respect users' privacy through tailored privacy support. Tailored privacy support is effective when risk is communicated alongside data request.

Studying all the possible factors influencing how users perceive information is a challenge. For example, the current research identified seven factors. However, three are assessed in Chapter 2 as critical factors, economic status, location tracking, and apps permission requests. Furthermore, the diversity of users' information sensitivity perceptions requires nuanced understanding across previously characterised user-categories as starting points. To initially understand the varying levels of sensitivity, the widely accepted Westin's privacy category was applied to characterise smartphone users into three categories. Additionally, participants were grouped by income levels. The income groups help to reveal the influence of economic status on users' perception. Doing this is based on the understanding that smartphone users differ, and the varying levels of information sensitivity perceptions help to tailor privacy support more accurately.

Tailoring privacy support is a countermeasure to the assumption of the *one-method-fits-all* approach. However, a tailoring approach should be informed by the views of smartphone users and by understanding the relationship between critical factors and user's privacy concern categories. Examining this relationship reveals the nuances in how information is perceived differently. Two critical factors (location tracking and app permission request) reflect the peculiarities of the context. Therefore, examining the

relationship accounts for the influence of the smartphone context and thus contextualises our findings. It is expected that knowledge from analysis of multiple factors will lead to a better understanding of how information sensitivity is distinctly influenced and how it should be correctly studied in this context. Against this background, this research proposes a middle range theory with the intent to support the formulation of tailored privacy for smartphone users.

This chapter provides the conclusion to the research. It highlights the contribution made and points out areas for future research. It begins (section 8.1) by presenting how the research questions were addressed in the study. Following this, the research contribution and its implications are discussed (see section 8.2). Subsequently, the limitations of the study are outlined in section 8.3. which also provided the directions for future research in sub-section 8.3.1 with emphasis on testing the propositions in a further quantitative study for enhancement. However, the quantitative testing is outside the scope of the current research. Finally, section 8.4 provides the closing remark to the research.

8.1 Answers to Research Questions

The study is conducted to answer the following research questions:

Question 1: *What are the critical factors that influence information sensitivity among smartphone users?*

This question is addressed in Chapter 2. It is revealed that economic status, location tracking and app permission requests are critical factors influencing how and why users perceive privacy risks and thus influencing how they perceive information as highly or less sensitive. The critical factors were justified on the basis that they yield implicit information about the user. Implicit information is information not explicitly disclosed but are inferred. In addition, some critical factors (location tracking and app permission request) allow the core characteristics of the smartphone ecosystem to directly affect users' privacy. Furthermore, another critical factor (economic status) influences decision making generally but has not been studied among smartphone users. Moreover, when a critical factor such as permission request is accepted by users, it allows direct access to users' information and in some cases, apps access data outside the permission granted.

Question 2: *What categories characterise privacy concerns among smartphone users whose personal data is collected via mobile applications?*

Our data analysis shows that smartphone users can be characterised into eight groups based on differences in perceived information sensitivity from the influences of users' economic status, location tracking and app permission requests. The question was fully addressed in chapters six and seven through insights obtained from the data analysis. The characterisations of smartphone users from our analysis are presented below:

1. Users that perceive identity information as highly sensitive are high-income, middle-income, and low-income privacy guardians.
2. Users that perceive identity information as less sensitive are high-income privacy pragmatists, privacy unconcerned, middle-income privacy pragmatists and privacy unconcerned, low-income privacy pragmatists and privacy unconcerned.
3. Users that perceive financial information as highly sensitive are high-income privacy guardians, privacy pragmatists and privacy unconcerned, middle-income privacy guardians and privacy pragmatists.
4. Users that perceive financial information as less sensitive are middle-income privacy unconcerned, low-income privacy guardians, privacy pragmatists, and privacy unconcerned.
5. Users that perceive location information as highly sensitive are privacy guardians.
6. Users that perceive location information as less sensitive are privacy pragmatists and privacy unconcerned.
7. Users whose perceived information sensitivity is heightened by app permission requests are privacy guardians.
8. Users who perceive apps permission request as a source of control over information requests thus perceiving app permission request with less sensitivity are privacy pragmatists and privacy unconcerned.

This finding is like Furini et al. (2019) who argues that smartphone users' response to app permission can be grouped into high and low sensitivity perceptions. However, we extend Furini et al. (2019) study by accounting for other factors such as economic

status and location tracking. Users economic status and privacy attributes intricately underpinned our categorisation.

Question 3: *How do the identified critical factors influence the perception of information sensitivity among smartphone users based on their characterised privacy concern?*

This research found that the critical factors (economic status, location tracking and app permission request) influence varying levels of information sensitivity across the characterised privacy categories. Regarding economic status, it was shown that the three privacy concern categories from high, middle, and low economic status perceive identity and financial information differently. Users perceive information as either highly sensitive or less sensitive. The details have been discussed in chapters six and seven. However, section 7.8 presents the summary that answers this research question.

Location tracking was addressed by showing that privacy guardians perceive location information as highly sensitive because of personal, situational, and profiling concerns. On the other hand, privacy pragmatists and privacy unconcerned users perceive location information as less sensitive due to higher influence of benefits and the convenience of using the smartphone. This was pointed out in chapter 7 (see Section 7.4).

Regarding app permission requests, it was found that privacy guardians perceive permission requests with high sensitivity because of concerns over malicious and unjustified requests. On the other hand, the privacy pragmatists and privacy unconcerned users perceive the request with less sensitivity because of a false perception of control that the permission requests triggers in them. This was addressed in chapter 7 (see Section 7.5).

Overall, the synthesis of the findings regarding the critical factors as mentioned above informed the theoretical propositions for understanding smartphone users' perception of information sensitivity in chapter 7 (see Section 7.7).

8.2 Research Contributions and Implications

This research has made theoretical and practical contributions to knowledge. Chapter 7 presented detailed discussions and tables that shows the emergent contributions. However, the key contributions to knowledge are summarised below. The theoretical contributions are:

1. One key contribution of this research is the eight new characterisations of smartphone users that shows differences in perceived information sensitivity. This is the first study as far this researcher knows, that points out this level of nuances relating to this important predictor of privacy decision making. Additionally, the study shows the underpinning reasons for each level of perceived information sensitivity.

2. This thesis contributes the understanding that smartphone users' economic status influence privacy concern to determine how different user-categories perceive information as highly or less sensitive. This contribution has been made in addressing research questions 2 and 3 above. This result shows that integrating users' economic status in studying the influences of privacy attributes on privacy decisions is important. The understanding of how economic status influences privacy decision making in the smartphone context was limited in the literature. The analysis of economic factor reveals four characterisations of smartphone users based on differences in perceived information sensitivity. Providing this understanding sheds light on the complexities surrounding privacy decisions. Moreover, studies that investigated the influence of users' economic status on privacy decisions are limited in privacy literature.

3. Another key contribution is the understanding that location tracking influences varying perception of information sensitivity among privacy guardians, privacy pragmatists and privacy unconcerned smartphone users. This is depicted in figure 7-1, which shows that location tracking makes privacy guardians to perceive location information as highly sensitive mainly because location information yields implicit information. On the other hand, location tracking makes pragmatists and privacy unconcerned users to perceive location information as less sensitive because they focus on the benefits of using the smartphone. The analysis of location tracking as a factor produced two

additional characterisations of smartphone users. This result is confirmed in table 7.4 which provides more details about this contribution.

4. This thesis contributes to a better understanding of the varying perceptions of information sensitivity regarding app permission requests from the perspectives of privacy guardians, privacy pragmatists and privacy unconcerned smartphone users. This result is revealed by addressing research question 3. This contribution confirms Furini et al. (2019) arguing that permission request triggers high and low perception of information sensitivity among smartphone users. However, our research extends Furini et al.(2019) study by showing not just how, but why permission request influences perception of information sensitivity among different categories of users. The inclusion of app permission request in our analysis produced two more characterisations of smartphone users. Thus, providing more nuanced understanding of the influence of app permission request.

5. A key contribution of this thesis is the middle range theory for understanding smartphone users' perception of information sensitivity (see Section 7.7). In developing the propositions, the researcher applied the recommendation by Hassan and Lowry (2015) and Hassan et al. (2019)**.** The middle range theory provides insight into the nuances surrounding how and why the three critical factors and the privacy concern categories influence users' perception of information sensitivity. This insight informed the characterisation of users into eight groups according to information sensitivity perceptions. This lays the foundation for tailored privacy that supports users based on the information cues that matches how information is perceived. Doing this enhance users' privacy in the smartphone context. Such understanding helps to avoid developing privacy support on the wrong premise - that all users perceive information the same way.

8.2.1 Practical contributions and the implications for practitioners

1. On the practical level, our findings shows how organisation's privacy policy could be designed. For example, linking Westin's characterisation with the influence of economic status, the nuances of users' worrisome collection of personal information have been revealed. The understanding of how different categories of users perceive privacy concern should be considered when designing privacy policies. In other words, using the insight this research provides, organisations can respond with right policies, products, and services to users' perception of information sensitivity.
2. This is the first study as far this researcher knows that clearly shows how smartphone users differs in terms of their responses to the concern for financial and identity information. Our findings provides the understanding of why and how the perceived information sensitivity varies between identity and financial information. This means that organisations can understand how to anticipate and respond differently based on both user categories and information types. This finding has important implication for practice because it considers the diversity of personal information and the diversity of privacy concerns. For example, the concern for safety of identity influences why high-income privacy guardians perceive information with high sensitivity. Confirming Solove (2003) contention, our findings further shows that the system of collection, dissemination, and use of personal information creates the "architectures of vulnerability," due to potential losses from identity theft. Additionally, this study reveals how distinct categories of users perceive vulnerability to identity theft and which categories of users are more likely to embrace PET (privacy enhancing technology) as a means of mitigating privacy risks (See section 7.2.1.1).

3. This research also makes practical contribution by showing how smartphone users who are privacy guardians could be accurately supported. Despite belonging to different economic status groups (income group), most privacy guardians perceive identity information as highly sensitive. Our findings shows that they require strong privacy-assurances that are specific enough to mitigate unwarranted disclosure. This study confirms that privacy-assurance mechanisms could be applied to increase privacy guardians' control of personal information by showing privacy customisation options in smartphone

settings. For example, the disabling of location history tracking and proxy control mechanisms contained in concise privacy statements and the use of assurance seals (See section 7.2.1.1).

4. This research confirms that malicious apps make disguised request to access users' resources. Such practices exacerbates privacy concern. However, our analysis found that PGs are more sensitive to these practices. Therefore, enhancing permission requests through better textual or symbolic description can reduce the perceived sensitivity of PGs towards app permissions. Furthermore, this study shows that developing tailored-permission requests that provides privacy assurances to different categories as Knijnenburg (2017) advocates could a counter measure to PGs high privacy concern. In highlighting this practical solution, our study deepens the privacy perception study by contributing the basis for applying nuanced app permission requests. Doing this advances the conversation from a general app request model to a more segmented, user-tailored model that should support every user's privacy (see subsection 7.2.1.3).

5. Finally, this research enhanced the RALC theory, making the publicity rule more applicable to smartphone users (see Section 7.6). This demonstrates how to tailor privacy communication by considering different levels of information sensitivity. Moreover, Mothersbaugh et al. (2012) argues that failure to account for information sensitivity affects the result of many research studies. Furthermore, how the three critical factors and the Westin's three privacy concern categories were integrated in a single qualitative analysis shows creativity in the application of Grounded Theory. In the analysis process shown in Chapter 6, the researcher compared various concepts and categories by identifying cues which point out differentiating levels of information sensitivity perceptions. This research is the first, as far as the researcher knows, to use Grounded Theory as a research method and methodology for comparing the influence of the critical factors across the Westins' three privacy concern categories.

To summarise our contributions, this research shows that privacy unconcerned users require empowerment to take the right action when they are presented with effective risk communication that combines information

request with user-education on how to disable access to information. Similarly, we expressed how privacy guardians and privacy pragmatists can be supported with succinct justification for information requests. Through the analysis of multiple factors in this research, nuances that could improve privacy mitigation practices were revealed. A privacy support model developed without a holistic understanding of the varying influences of the critical factors from the distinct categories of users to whom the model will be applied could be based on assumptions.

Additionally, as the research shows the nuances in users' perception of information sensitivity, it has implication for predicting users' responses to privacy risks. This is because a value of understanding perception of information sensitivity is the predictability of privacy decisions (Furini et al., 2019; Mothersbaugh et al., 2012).

Studies shows that perception of information sensitivity is context dependent (Bansal et al., 2016; Knijnenburg and Kobsa, 2013) and high sensitivity perceptions are underlying obstacles to the uptake of mobile applications (Guinchard, 2020; Kokkoris and Kamleitner, 2020; Kulyk et al., 2019). Although the uptake of some apps like the UK COVID19 Track and Trace app could be government-mandated, users still require tailored support to encourage its use. Therefore, the type of understanding provided by this research can be applied to support uptake and usage of useful apps.

Finally, as shown in table 7.6, most studies on information sensitivity focused broadly on internet users without particular attention to the smartphone context. Therefore, our research draws attention to the smartphone context and extends the understanding of contextual and economic status influence on privacy; it points out the relationship between the critical factors and characterised privacy attributes – thus providing incentive for more research around these factors.

8.3 Limitations of Research

The research is subject to some limitations, that future research should take into consideration. The following are the limitations reflected on:

1. **The exclusion of privacy-related knowledge as an explicit factor in the analysis**

Studies show that individuals' level of privacy-related knowledge influence the perception of information sensitivity (Bartsch and Dienlin, 2016). Although basic privacy literacy is indirectly integrated in the analysis, the current study is limited to an analysis of three explicit critical factors, excluding privacy-related knowledge. However, this limitation is moderated by the sampling techniques (convenience and purposive sampling) that purposefully selected only participants that have at least a first-degree education. Studies (Surma et al., 2012; Turow et al., 2008) show that graduate level education provides basic privacy literacy (see section 5.11). Despite this sampling approach, it cannot be completely ruled out that a relevant factor may have been excluded. Therefore, this research cannot be generalised to the 60% of the UK population that do not have a university or basic privacy knowledge.

2. The limitations imposed by methodology

Conducting the research through Nonprobability convenience and purposive sampling techniques implies that the research sample may not be an all-encompassing representation of the distinct categories of smartphone users. Arguably, probability sampling is unfitting for qualitative studies because it lends itself to statistical computations. Furthermore, the research applied the grounded theory approach that allows participants to be chosen through the theoretical sampling method. However, the size of the chosen sample for each privacy concern category is quite small compared with sample sizes in quantitative research. To offset this limitation, Hassan and Lowry (2015) and Hassan et al. (2019) argues that middle range theorist should seek further deductive testing in a quantitative study. Moreover, qualitative research does not try to be formally representative.

3. **Limitation of generalisability**

The empirical study participants were all university graduates. Studies show that possessing a university degree increases individuals' privacy risk perception (Bartsch and Dienlin, 2016; Turow et al., 2008). Therefore, the generalisability of this research findings is limited only to similar populations.

4. Limitations regarding "tailored privacy"

Presently, there are no clear incentives for companies who build apps to provide tailored privacy support for users. This scenario limits the implementation of tailored privacy in the smartphone ecosystem. However, when companies understand the corporate and reputational benefits that they can derive from being “socially and privacy” responsible, then positioning themselves as privacy champions may enhance corporate image.

8.3.1 Future Research

The factors influencing the perception of information sensitivity are complex. Therefore, researcher envisions several other extensions of the current work. Importantly, the middle range theory for enabling the formulation of tailored privacy support should be tested in a wider quantitative study. Doing this will enhance validity and applicability by combining the strengths of both qualitative and quantitative studies (Kaplan and Duchon, 1988; Venkatesh et al., 2013). Moreover, middle range theories are tentative propositions that should be deductively tested (Corbin and Strauss, 1990; Hassan et al., 2019b; Hassan and Lowry, 2015). To further enhance the propositions, future study should integrate privacy-related knowledge as an explicit factor in the analysis as well as including non-university graduates as research participants. Additionally, even the implementation of a tailored privacy described in Chapter 7 (see Section 7.2.1.3) is still limited; a true test of the benefits would be confirmed in studies where experimental and control groups representing each category of users are observed. Future work should implement a tailored privacy support in such a study. Additionally, studies that points out incentives for companies who build apps to implement tailored privacy are required.

8.4 Closing Remark

Smartphone users cannot be accurately supported without understanding the privacy-related categories that characterise users whose personal information are at risk. Since users perceive and respond to privacy risks differently, a clear understanding of the varying levels of perceived information sensitivity is also needed. However, prior studies have addressed information sensitivity by showing the high and low levels of sensitivity perceptions online but did not fully explain why the levels varies in the smartphone context. Additionally, prior studies addressed the necessity of

understanding the context-dependencies of information sensitivity without explaining how economic-status and other critical-factors shape information sensitivity among smartphone users. Therefore, devoting attention to unearth these nuances provides the foundation for tailored privacy support in the smartphone context.

This research was conducted as an interpretivist Grounded Theory study. This approach was chosen as it allows the gaining of in-depth understanding of perceived information sensitivity. Particularly when exploring how and why different categories of smartphone users perceive privacy risks. The researcher had to rely on an intuitive and self-learning process to analyse the empirical data when extant literature did not provide fitting example. However, the prescribed systematic procedures of the Straussian strand of Grounded Theory have been followed to categorise the developing concepts up to the point of summarising them into core categories. The core categories expressed the phenomenon regarding the critical factors and their influences across the characterised privacy categories. At the end, the researcher acquired valuable expertise through the analysis process and developed the testable theoretical propositions that could inform further studies.

References

Abakouy, R., En-naimi, E.M., Haddadi, A.E., Lotfi, E., 2019. Data-driven marketing: how machine learning will improve decision-making for marketers, in: Proceedings of the 4th International Conference on Smart City Applications - SCA '19. Presented at the the 4th International Conference, ACM Press, Casablanca, Morocco, pp. 1–5. https://doi.org/10.1145/3368756.3369024

Abbas, R., Michael, K., Michael, M., 2014. The regulatory considerations and ethical dilemmas of location-based services (LBS): A literature review. Inf. Technol. People 27, 2–20. https://doi.org/10.1108/ITP-12-2012-0156

Abbas, R., Michael, K., Michael, M.G., Aloudat, A., 2011. Emerging Forms of Covert Surveillance Using GPS-Enabled Devices: J. Cases Inf. Technol. 13, 19–33. https://doi.org/10.4018/JCIT.2011040102

Abdulazim, T., Abdelgawad, H., Habib, K., Abdulhai, B., 2013. Using smartphones and sensor technologies to automate collection of travel data. Transp. Res. Rec. 44–52. https://doi.org/10.3141/2383-06

Abubaker, H., Shamsuddin, S.M., Ali, A., 2018. Analytics on malicious android applications. Int. J. Adv. Soft Comput. Its Appl. 10, 106–118.

Ackerman, M.S., Cranor, L.F., Reagle, J., 1999. Privacy in e-commerce: examining user scenarios and privacy preferences, in: Proceedings of the 1st ACM Conference on Electronic Commerce - EC '99. Presented at the the 1st ACM conference, ACM Press, Denver, Colorado, United States, pp. 1–8. https://doi.org/10.1145/336992.336995

Acquisti, A., 2004a. Privacy in electronic commerce and the economics of immediate gratification, in: Proceedings of the 5th ACM Conference on Electronic Commerce. ACM, pp. 21–29.

Acquisti, A., 2004b. Privacy and security of personal information, in: Economics of Information Security. Springer, pp. 179–186.

Acquisti, A., Brandimarte, L., Loewenstein, G., 2015. Privacy and human behavior in the age of information. Science 347, 509–514. https://doi.org/10.1126/science.aaa1465

Acquisti, A., Sleeper, M., Wang, Y., Wilson, S., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L.F., Komanduri, S., Leon, P.G., Sadeh, N., Schaub, F., 2017. Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. ACM Comput. Surv. 50, 1–41. https://doi.org/10.1145/3054926

Acquisti, A., Taylor, C., Wagman, L., 2016. The Economics of Privacy. J. Econ. Lit. 54, 442–492. https://doi.org/10.1257/jel.54.2.442

Acquisti, Alessandro, Taylor, C.R., Wagman, L., 2015. The Economics of Privacy (SSRN Scholarly Paper No. ID 2580411). Social Science Research Network, Rochester, NY.

Acquisti, Grossklags, J., 2005. Privacy and rationality in individual decision making. IEEE Secur. Priv. Mag. 3, 26–33. https://doi.org/10.1109/MSP.2005.22

Acquisti, John, L.K., Loewenstein, G., 2013. What is privacy worth? J. Leg. Stud. 42, 249–274. https://doi.org/10.1086/671754

Ahmed, R., Robinson, R., Elsony, A., Thomson, R., Bertel Squire, S., Malmborg, R., Burney, P., Mortimer, K., 2018. A comparison of smartphone and paper data-collection tools in the Burden of Obstructive Lung Disease (BOLD) study in Gezira state, Sudan. PLoS ONE 13. https://doi.org/10.1371/journal.pone.0193917

Aicardi, C., Fothergill, B.T., Rainey, S., Stahl, B.C., Harris, E., 2018. Accompanying technology development in the Human Brain Project: From foresight to ethics management. Futures. https://doi.org/10.1016/j.futures.2018.01.005

Ajzen, I., 1985. From Intentions to Actions: A Theory of Planned Behavior, in: Kuhl, J., Beckmann, J. (Eds.), Action Control. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 11–39. https://doi.org/10.1007/978-3-642-69746-3_2

Alammar, F., Intezari, A., Cardow, A., J. Pauleen, D., 2019. Grounded Theory in Practice: Novice Researchers' Choice Between Straussian and Glaserian. J. Manag. Inq. 28, 228–245. https://doi.org/10.1177/1056492618770743

Alazab, Moutaz, Alazab, Mamoun, Shalaginov, A., Mesleh, A., Awajan, A., 2020. Intelligent mobile malware detection using permission requests and API calls. Future Gener. Comput. Syst. 107, 509–521. https://doi.org/10.1016/j.future.2020.02.002

Alexander, L., Jiang, S., Murga, M., González, M.C., 2015. Origin–destination trips by purpose and time of day inferred from mobile phone data. Transp. Res. Part C Emerg. Technol. 58, 240–250. https://doi.org/10.1016/j.trc.2015.02.018

Almuhimedi, H., Schaub, F., Sadeh, N., Adjerid, I., Acquisti, A., Gluck, J., Cranor, L.F., Agarwal, Y., 2015. Your Location has been Shared 5,398 Times!: A Field Study on Mobile App Privacy Nudging. ACM Press, pp. 787–796. https://doi.org/10.1145/2702123.2702210

Aloudat, A., Michael, K., Chen, X., Al-Debei, M.M., 2014. Social acceptance of location-based mobile government services for emergency management. Telemat. Inform. 31, 153–171. https://doi.org/10.1016/j.tele.2013.02.002

Alvesson, M., Deetz, S., 2000. Doing Critical Management Research. SAGE Publications Ltd, 6 Bonhill Street, London England EC2A 4PU United Kingdom. https://doi.org/10.4135/9781849208918

Amit, M., Kimhi, H., Bader, T., Chen, J., Glassberg, E., Benov, A., 2020. Mass-surveillance technologies to fight coronavirus spread: the case of Israel. Nat. Med. 26, 1167–1169. https://doi.org/10.1038/s41591-020-0927-z

Anand, G., Larson, E.C., Mahoney, J.T., 2020. Thomas Kuhn on Paradigms. Prod. Oper. Manag. 29, 1650–1657.

Anderson, C., Baskerville, R.L., Kaul, M., 2017. Information Security Control Theory: Achieving a Sustainable Reconciliation Between Sharing and Protecting the Privacy of Information. J. Manag. Inf. Syst. 34, 1082–1112. https://doi.org/10.1080/07421222.2017.1394063

Angulo, J., Fischer-Hübner, S., Wästlund, E., Pulls, T., 2012. Towards usable privacy policy display and management. Inf. Manag. Comput. Secur. 20, 4–17. https://doi.org/10.1108/09685221211219155

Anic, I.-D., Škare, V., Milaković, I.K., 2019. The determinants and effects of online privacy concerns in the context of e-commerce. Electron. Commer. Res. Appl. 36, 100868.

Armando, A., Bezzi, M., Metoui, N., Sabetta, A., 2015. Risk-Aware Information Disclosure, in: GarciaAlfaro, J., HerreraJoancomarti, J., Lupu, E., Posegga, J., Aldini, A., Martinelli, F., Suri, N. (Eds.), Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance. pp. 266–276.

Ashford, W., 2018. Most Britons concerned about personal data sharing. ComputerWeekly.com.

Assemi, B., Jafarzadeh, H., Mesbah, M., Hickman, M., 2018. Participants' perceptions of smartphone travel surveys. Transp. Res. Part F Traffic Psychol. Behav. 54, 338–348. https://doi.org/10.1016/j.trf.2018.02.005

Atkinson, S., 1994. Rethinking the Principles and Practice of Action Research: the tensions for the teacher-researcher. Educ. Action Res. 2, 383–401. https://doi.org/10.1080/0965079940020306

Avison, D., Kock, N., Malaurent, J., 2017. Special Issue: Action Research in Information Systems. J. Manag. Inf. Syst. 34, 630–632. https://doi.org/10.1080/07421222.2017.1372995

Babbie, E.R., 2007. The practice of social research. Cengage Learning.

Bacharach, S.B., 1989. Organizational theories: Some criteria for evaluation. Acad. Manage. Rev. 14, 496–515.

Balebako, R., Cranor, L., 2014. Improving App Privacy: Nudging App Developers to Protect User Privacy. IEEE Secur. Priv. 12, 55–58. https://doi.org/10.1109/MSP.2014.70

Balebako, R., Leon, P.G., Almuhimedi, H., Kelley, P.G., Mugan, J., Acquisti, A., Cranor, L.F., Sadeh, N., 2011. Nudging users towards privacy on mobile devices. Presented at the CEUR Workshop Proceedings, pp. 23–26.

Banovic, N., Brant, C., Mankoff, J., Dey, A., 2014. ProactiveTasks: the short of mobile device use sessions, in: Proceedings of the 16th International Conference on Human-Computer Interaction with Mobile Devices & Services - MobileHCI '14. Presented at the the 16th international conference, ACM Press, Toronto, ON, Canada, pp. 243–252. https://doi.org/10.1145/2628363.2628380

Bansal, G., Zahedi, F. "Mariam", Gefen, D., 2010a. The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. Decis. Support Syst. 49, 138–150. https://doi.org/10.1016/j.dss.2010.01.010

Bansal, G., Zahedi, F.M., Gefen, D., 2016. Do context and personality matter? Trust and privacy concerns in disclosing private information online. Inf. Manage. 53, 1–21. https://doi.org/10.1016/j.im.2015.08.001

Bansal, G., Zahedi, F.M., Gefen, D., 2010b. The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. Decis. Support Syst. 49, 138–150. https://doi.org/10.1016/j.dss.2010.01.010

Bansal, Zahedi, F.M., Gefen, D., 2016. Do context and personality matter? Trust and privacy concerns in disclosing private information online. Inf. Manage. 53, 1–21. https://doi.org/10.1016/j.im.2015.08.001

Barhamgi, M., Perera, C., Ghedira, C., Benslimane, D., 2018. User-centric Privacy Engineering for the Internet of Things. IEEE Cloud Comput. 5, 47–57. https://doi.org/10.1109/MCC.2018.053711666

Barth, S., de Jong, M.D.T., 2017. The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. Telemat. Inform. 34, 1038–1058. https://doi.org/10.1016/j.tele.2017.04.013

Bartsch, M., Dienlin, T., 2016. Control your Facebook: An analysis of online privacy literacy. Comput. Hum. Behav. 56, 147–154. https://doi.org/10.1016/j.chb.2015.11.022

Baruh, L., Secinti, E., Cemalcilar, Z., 2017. Online Privacy Concerns and Privacy Management: A Meta-Analytical Review: Privacy Concerns Meta-Analysis. J. Commun. 67, 26–53. https://doi.org/10.1111/jcom.12276

Beardsley, E.L., 2017. Privacy: Autonomy and Selective Disclosure, in: Pennock, J.R., Chapman, J.W. (Eds.), Privacy & Personality. Routledge, pp. 56–70. https://doi.org/10.4324/9781315127439-3

Bélanger, Crossler, 2011. Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. MIS Q. 35, 1017. https://doi.org/10.2307/41409971

Beldad, A., de Jong, M., Steehouder, M., 2011. A Comprehensive Theoretical Framework for Personal Information-Related Behaviors on the Internet. Inf. Soc. 27, 220–232. https://doi.org/10.1080/01972243.2011.583802

Beldad, A.D., 2015. Sharing to be sociable, posting to be popular: Factors influencing non-static personal information disclosure on Facebook among young Dutch users. Int. J. Web Based Communities 11, 357–374. https://doi.org/10.1504/IJWBC.2015.072132

Belgrave, L.L., Seide, K., 2019. Grounded theory methodology: principles and practices, in: Handbook of Research Methods in Health Social Sciences. Springer Singapore, pp. 299–316.

Benton, K., Camp, L.J., Garg, V., 2013. Studying the effectiveness of android application permissions requests, in: 2013 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops). Presented at the 2013 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), pp. 291–296. https://doi.org/10.1109/PerComW.2013.6529497

Berenguer, A., Goncalves, J., Hosio, S., Ferreira, D., Anagnostopoulos, T., Kostakos, V., 2017. Are Smartphones Ubiquitous?: An in-depth survey of smartphone adoption by seniors. IEEE Consum. Electron. Mag. 6, 104–110. https://doi.org/10.1109/MCE.2016.2614524

Bhatnagar, A., Ghose, S., 2004. Segmenting consumers based on the benefits and risks of Internet shopping. J. Bus. Res., Mobility and Markets: Emerging Outlines of M-Commerce 57, 1352–1360. https://doi.org/10.1016/S0148-2963(03)00067-5

Bhih, A.A., Johnson, P., Randles, M., 2016. Diversity in Smartphone Usage, in: Proceedings of the 17th International Conference on Computer Systems and Technologies 2016 - CompSysTech '16. Presented at the the 17th International Conference, ACM Press, Palermo, Italy, pp. 81–88. https://doi.org/10.1145/2983468.2983496

Blau, P.M., 1997. On limitations of rational choice theory for sociology. Am. Sociol. Wash. 28, 16–21. http://dx.doi.org.proxy.library.dmu.ac.uk/10.1007/s12108-997-1003-6

Boateng, F.L., Panford, J.K., Hayfron-Acquah, J.B., 2019. Vulnerabilities in Android Apps Permissions. Int. J. Comput. Sci. Inf. Secur. IJCSIS 17.

Bösch, C., Erb, B., Kargl, F., Kopp, H., Pfattheicher, S., 2016. Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns. Proc. Priv. Enhancing Technol. 2016. https://doi.org/10.1515/popets-2016-0038

Bouwman, H., de Reuver, M., Heerschap, N., Verkasalo, H., 2013. Opportunities and problems with automated data collection via smartphones. Mob. Media Commun. 1, 63–68. https://doi.org/10.1177/2050157912464492

Boyles, J.L., Smith, A., Madden, M., 2012. Privacy and Data Management on Mobile Devices. Pew Res. Cent. Internet Sci. Tech. URL http://www.pewinternet.org/2012/09/05/privacy-and-data-management-on-mobile-devices/ (accessed 3.3.16).

Braun, V., Clarke, V., 2013. Successful qualitative research: a practical guide for beginners. SAGE, Los Angeles.

Brough, A.R., Martin, K.D., 2020. Critical roles of knowledge and motivation in privacy research. Curr. Opin. Psychol. 31, 11–15. https://doi.org/10.1016/j.copsyc.2019.06.021

Bryman, A., 2007. The Research Question in Social Research: What is its Role? Int. J. Soc. Res. Methodol. 10, 5–20. https://doi.org/10.1080/13645570600655282

Bryman, A., Bell, E., 2015a. Business research methods, Fourth edition. ed. Oxford University Press, Cambridge, United Kingdom ; New York, NY, United States of America.

Bryman, A., Bell, E., 2015b. Business research methods, Fourth edition. ed. Oxford University Press, Cambridge, United Kingdom ; New York, NY, United States of America.

Burrell, G., Morgan, 1979. Morgan, 1979. Sociological Paradigms and Organizational Analysis: Elements of the Sociology of Corporate Life. London: Heineman.

Cabalquinto, E., Hutchins, B., 2020. '"It should allow me to opt in or opt out": Investigating smartphone use and the contending attitudes of commuters towards geolocation data collection. Telemat. Inform. 51, 101403. https://doi.org/10.1016/j.tele.2020.101403

Cai, H., Zhu, Y., Feng, Z., Zhu, H., Yu, J., Cao, J., 2018. Truthful incentive mechanisms for mobile crowd sensing with dynamic smartphones. Comput. Netw. 141, 1–16. https://doi.org/10.1016/j.comnet.2018.05.016

Can, Z., Demirbas, M., 2015. Smartphone-based data collection from wireless sensor networks in an urban environment. J. Netw. Comput. Appl. 58, 208–216. https://doi.org/10.1016/j.jnca.2015.08.013

Capistrano, E., Chen, J.V., 2015. Information privacy policies: The effects of policy characteristics and online experience. Comput. Stand. Interfaces 42, 24–31. https://doi.org/10.1016/j.csi.2015.04.001

Carrascal, J.P., Riederer, C., Erramilli, V., Cherubini, M., de Oliveira, R., 2013. Your browsing behavior for a big mac: Economics of personal information online, in: Proceedings of the 22nd International Conference on World Wide Web. International World Wide Web Conferences Steering Committee, pp. 189–200.

Cato, K.D., Bockting, W., Larson, E., 2016. Did i tell you that? Ethical issues related to using computational methods to discover non-disclosed patient characteristics. J. Empir. Res. Hum. Res. Ethics 11, 214–219. https://doi.org/10.1177/1556264616661611

Cecere, G., Le Guel, F., Soulié, N., 2015. Perceived Internet privacy concerns on social networks in Europe. Technol. Forecast. Soc. Change 96, 277–287. https://doi.org/10.1016/j.techfore.2015.01.021

Center, E.P.I., 2002. EPIC - Public Opinion on Privacy [WWW Document]. Alan Westin Priv. Fundam. URL https://epic.org/privacy/survey/ (accessed 8.18.20).

Cheng, N., Oscar Wang, X., Cheng, W., Mohapatra, P., Seneviratne, A., 2013. Characterizing privacy leakage of public WiFi networks for users on travel. IEEE, pp. 2769–2777. https://doi.org/10.1109/INFCOM.2013.6567086

Cheung, A.S.Y., 2014. Location privacy: The challenges of mobile service devices. Comput. Law Secur. Rev. 30, 41–54. https://doi.org/10.1016/j.clsr.2013.11.005

Chirban, J.T., 1996. Interviewing in depth: the interactive-relational approach. Sage Publications, Thousand Oaks, Calif.

Choi, J., Sung, W., Choi, C., Kim, P., 2015. Personal information leakage detection method using the inference-based access control model on the Android platform. Pervasive Mob. Comput. 24, 138–149. https://doi.org/10.1016/j.pmcj.2015.06.005

Choi, S., 2016a. The flipside of ubiquitous connectivity enabled by smartphone-based social networking service: Social presence and privacy concern. Comput. Hum. Behav. 65, 325–333. https://doi.org/10.1016/j.chb.2016.08.039

Choi, S., 2016b. The flipside of ubiquitous connectivity enabled by smartphone-based social networking service: Social presence and privacy concern. Comput. Hum. Behav. 65, 325–333. https://doi.org/10.1016/j.chb.2016.08.039

Chua, W.F., 1986. Radical developments in accounting thought. Account. Rev. 601–632.

Chun Tie, Y., Birks, M., Francis, K., 2019. Grounded theory research: A design framework for novice researchers. SAGE Open Med. 7, 205031211882292. https://doi.org/10.1177/2050312118822927

Church, K., Ferreira, D., Banovic, N., Lyons, K., 2015. Understanding the Challenges of Mobile Phone Usage Data, in: Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services - MobileHCI '15. Presented at the the 17th International Conference, ACM Press, Copenhagen, Denmark, pp. 504–514. https://doi.org/10.1145/2785830.2785891

Chuttur, M., 2009. Overview of the Technology Acceptance Model: Origins, Developments and Future Directions. Sprouts Content.

CNIL, 2019. The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC | CNIL [WWW Document]. CNIL's Restricted Comm. Impos. Financ. Penal. 50 Million Euros GOOGLE LLC. URL https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc (accessed 12.14.20).

Conti, N., Jennett, C., Maestre, J., Sasse, M.A., Street, G., WC, L., 2012. When Did My Mobile Turn Into A 'Sellphone'? A study of consumer responses to tailored smartphone ads 6.

Corbetta, P., 2003. Social research: theory, methods and techniques. SAGE Publications, London ; Thousand Oaks, Calif.

Corbin, J.M., Strauss, A., 1990. Grounded theory research: Procedures, canons, and evaluative criteria. Qual. Sociol. 13, 3–21. https://doi.org/10.1007/BF00988593

Corley, K.G., 2015. A Commentary on "What Grounded Theory Is…": Engaging a Phenomenon from the Perspective of Those Living it. Organ. Res. Methods 18, 600–605. https://doi.org/10.1177/1094428115574747

Cornet, V.P., Holden, R.J., 2018. Systematic review of smartphone-based passive sensing for health and wellbeing. J. Biomed. Inform. 77, 120–132. https://doi.org/10.1016/j.jbi.2017.12.008

Cottrill, C.D., "Vonu" Thakuriah, P., 2015. Location privacy preferences: A survey-based analysis of consumer awareness, trade-off and decision-making. Transp. Res. Part C Emerg. Technol. 56, 132–148. https://doi.org/10.1016/j.trc.2015.04.005

Council of Europe, 2010. European Convention on Human Rights.

Couper, M.P., Gremel, G., Axinn, W., Guyer, H., Wagner, J., West, B.T., 2018. New options for national population surveys: The implications of internet and smartphone coverage. Soc. Sci. Res. 73, 221–235. https://doi.org/10.1016/j.ssresearch.2018.03.008

Crema, C., Depari, A., Flammini, A., Sisinni, E., Vezzoli, A., Bellagente, P., 2017. Virtual Respiratory Rate Sensors: An Example of A Smartphone-Based Integrated and Multiparametric mHealth Gateway. IEEE Trans. Instrum. Meas. 66, 2456–2463. https://doi.org/10.1109/TIM.2017.2707838

Creswell, J.W., 2003. Research design: qualitative, quantitative, and mixed method approaches, 2nd ed. ed. Sage Publications, Thousand Oaks, Calif.

Creswell, J.W., 1998. Qualitative inquiry and research design: choosing among five traditions. Sage Publications, Thousand Oaks, Calif.

Creswell, J.W., Poth, C.N., 2018. Qualitative inquiry & research design: choosing among five approaches, Fourth edition. ed. SAGE, Los Angeles.

Crotty, M., 1998. The foundations of social research: Meaning and perspective in the research process. Sage.

Crowther, D., Lancaster, G., 2008. Research Methods: A Concise Introduction to Research in Management and Business Consultancy. Butterworth-Heinemann.

Cvrcek, D., Kumpost, M., Matyas, V., Danezis, G., 2006. A study on the value of location privacy, in: Proceedings of the 5th ACM Workshop on Privacy in Electronic Society. Presented at the WPES '06 Proceedings of the 5th ACM workshop on Privacy in electronic society, ACM, New York, pp. 109–118.

Da Veiga, A., Ophoff, J., 2020. Concern for Information Privacy: A Cross-Nation Study of the United Kingdom and South Africa, in: Clarke, N., Furnell, S. (Eds.), Human Aspects of Information Security and Assurance, IFIP Advances in Information and Communication Technology. Springer International Publishing, Cham, pp. 16–29. https://doi.org/10.1007/978-3-030-57404-8_2

Davies, C., Fisher, M., others, 2018. Understanding research paradigms. J. Australas. Rehabil. Nurses Assoc. 21, 21.

De Cleen, B., Glynos, J., Mondon, A., 2018. Critical research on populism: Nine rules of engagement. Organization 25, 649–661. https://doi.org/10.1177/1350508418768053

De Cristofaro, E., Durussel, A., Aad, I., 2011. Reclaiming Privacy for Smartphone Applications. 2011 Ieee Int. Conf. Pervasive Comput. Commun. Percom 2011 84–92.

Degirmenci, K., 2020. Mobile users' information privacy concerns and the role of app permission requests. Int. J. Inf. Manag. 50, 261–272.

Del Rosario, M.B., Wang, K., Wang, J., Liu, Y., Brodie, M., Delbaere, K., Lovell, N.H., Lord, S.R., Redmond, S.J., 2014. A comparison of activity classification in younger and older cohorts using a smartphone. Physiol. Meas. 35, 2269–2286. https://doi.org/10.1088/0967-3334/35/11/2269

Dempsey, L., Dowling, M., Larkin, P., Murphy, K., 2016. Sensitive Interviewing in Qualitative Research. Res. Nurs. Health 39, 480–490. https://doi.org/10.1002/nur.21743

Denscombe, M., 2003. The Good Research Guide: For Small-Scale Social Research Projects., 2nd edition. ed. Open University Press., Buckingham.

Denzin, N.K., Lincoln, Y.S. (Eds.), 2000. Handbook of qualitative research, 2nd ed. ed. Sage Publications, Thousand Oaks, Calif.

Dhawan, S., Singh, K., Goel, S., 2014. Impact of Privacy Attitude, Concern and Awareness on Use of Online Social Networking. 2014 5th Int. Conf. Conflu. Gener. Inf. Technol. Summit Conflu. 14–17.

DiCicco-Bloom, B., Crabtree, B.F., 2006. The qualitative research interview. Med. Educ. 40, 314–321. https://doi.org/10.1111/j.1365-2929.2006.02418.x

Dilthey, W., 1883. An introduction to the human studies. Selected Writings. Cambridge: Cambridge University Press.

Dinev, T., 2014. Why would we care about privacy? Eur. J. Inf. Syst. 23, 97–102. https://doi.org/10.1057/ejis.2014.1

Dinev, T., Hart, P., 2006. An Extended Privacy Calculus Model for E-Commerce Transactions. Inf. Syst. Res. 17, 61–80. https://doi.org/10.1287/isre.1060.0080

Do, T.M.T., Blom, J., Gatica-Perez, D., 2011. Smartphone usage in the wild: a large-scale analysis of applications and context, in: Proceedings of the 13th International Conference on Multimodal Interfaces - ICMI '11. Presented at the the 13th international conference, ACM Press, Alicante, Spain, p. 353. https://doi.org/10.1145/2070481.2070550

Dobson, J.E., Fisher, P.F., 2003. Geoslavery. IEEE Technol. Soc. Mag. 22, 47–52. https://doi.org/10.1109/MTAS.2003.1188276

Doherty, N.F., Tajuddin, S.T., 2018. Towards a user-centric theory of value-driven information security compliance. Inf. Technol. People 31, 348–367. https://doi.org/10.1108/ITP-08-2016-0194

Dolnicar, S., Jordaan, Y., 2007. A Market-Oriented Approach to Responsibly Managing Information Privacy Concerns in Direct Marketing. J. Advert. 36, 123–149. https://doi.org/10.2753/JOA0091-3367360209

Dudovskiy, J., 2016. Interpretivism (interpretivist). Res. Methodol. URL http://research-methodology.net/research-philosophy/interpretivism/ (accessed 6.7.16).

Eckhoff, D., Wagner, I., 2018. Privacy in the Smart City—Applications, Technologies, Challenges, and Solutions. IEEE Commun. Surv. Tutor. 20, 489–516. https://doi.org/10.1109/COMST.2017.2748998

Eisenhart, M., 1991. Conceptual frameworks for research circa 1991: Ideas from a cultural anthropologist; implications for mathematics education rese.

Falaki, H., Mahajan, R., Kandula, S., Lymberopoulos, D., Govindan, R., Estrin, D., 2010. Diversity in smartphone usage, in: Proceedings of the 8th International Conference on Mobile Systems, Applications, and Services - MobiSys '10. Presented at the the 8th international conference, ACM Press, San Francisco, California, USA, p. 179. https://doi.org/10.1145/1814433.1814453

Falconer, D.J., Mackay, D.R., 1999. The Key to the Mixed Method Dilemma. Presented at the PROC. 10 TH AUSTRALASIAN CONFERENCE ON INFORMATION SYSTEMS.

Fawaz, K., Shin, K.G., 2014. Location Privacy Protection for Smartphone Users. ACM Press, pp. 239–250. https://doi.org/10.1145/2660267.2660270

Felt, A.P., Ha, E., Egelman, S., Haney, A., Chin, E., Wagner, D., 2012. Android Permissions: User Attention, Comprehension, and Behavior, in: Proceedings of the Eighth Symposium on Usable Privacy and Security, SOUPS '12. ACM, New York, NY, USA, p. 3:1-3:14. https://doi.org/10.1145/2335356.2335360

Fife, E., Orjuela, J., 2012. The privacy calculus: Mobile apps and user perceptions of privacy and security. Int. J. Eng. Bus. Manag. 4, 1–10. https://doi.org/10.5772/51645

Fried, C., 1984. "Privacy" in Philosophical dimensions of privacy: an anthology. Cambridge University Press, Cambridge [Cambridgeshire] ; New York.

Fried, C., 1968. Privacy. Yale Law J. 77, 475. https://doi.org/10.2307/794941

Fry, M., Curtis, K., Considine, J., Shaban, R.Z., 2017. Using observation to collect data in emergency research. Australas. Emerg. Nurs. J. 20, 25–30. https://doi.org/10.1016/j.aenj.2017.01.001

Furini, M., Mirri, S., Montangero, M., Prandi, C., 2020. Privacy Perception when Using Smartphone Applications. Mob. Netw. Appl. 25, 1055–1061. https://doi.org/10.1007/s11036-020-01529-z

Furini, M., Mirri, S., Montangero, M., Prandi, C., 2019. Privacy perception and user behavior in the mobile ecosystem, in: Proceedings of the 5th EAI International Conference on Smart Objects and Technologies for Social Good. Presented at the GoodTechs '19: EAI International Conference on Smart Objects and Technologies for Social Good, ACM, Valencia Spain, pp. 177–182. https://doi.org/10.1145/3342428.3342690

Fusco, S.J., Abbas, R., Michael, K., Aloudat, A., 2012. Location-Based Social Networking: Impact on Trust in Relationships. IEEE Technol. Soc. Mag. 31, 39–50. https://doi.org/10.1109/MTS.2012.2196340

Gao, J., Zhang, Y.-C., Zhou, T., 2019. Computational socioeconomics. Phys. Rep. 817, 1–104. https://doi.org/10.1016/j.physrep.2019.05.002

Garrison, L., Hastak, M., Hogarth, J.M., Kleimann, S., Levy, A.S., 2012. Designing Evidence-based Disclosures: A Case Study of Financial Privacy Notices. J. Consum. Aff. 46, 204–234. https://doi.org/10.1111/j.1745-6606.2012.01226.x

Gates, C.S., Chen, J., Li, N., Proctor, R.W., 2014. Effective Risk Communication for Android Apps. IEEE Trans. Dependable Secure Comput. 11, 252–265. https://doi.org/10.1109/TDSC.2013.58

Gibbons, M.T., 1987. Introduction: The politics of interpretation. Interpret. Polit. 1–31.

Gibson, D., 1987. Blair/Geselowitz, Michael N., The Evolution of Complex Society in Late Prehistoric Europe: Toward a Paradigm. DiesHgg Tribe Polity 3–37.

Gioia, D.A., Corley, K.G., Hamilton, A.L., 2013. Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology. Organ. Res. Methods 16, 15–31. https://doi.org/10.1177/1094428112452151

Glaser, B.G., Strauss, A.L., 2009. The discovery of grounded theory: strategies for qualitative research, 4. paperback printing. ed. Aldine, New Brunswick.

Goel, S., Hofman, J., Sirer, M.I., 2012. Who does what on the Web: Studying Web browsing behavior at scale, in: International Conference on Weblogs and Social Media. pp. 130–137.

Gotz, F.M., Stieger, S., Reips, U.-D., 2017. Users of the main smartphone operating systems (iOS, Android) differ only little in personality. PLoS ONE 12. https://doi.org/10.1371/journal.pone.0176921

Goulding, C., 2002. Grounded theory: a practical guide for management, business and market researchers. SAGE, London ; Thousand Oaks, Calif.

Group, V.T.C., 2020. Data Privacy Day 2020 : What is Your Data Net Worth? Vantage Technol. Consult. Group. URL https://www.vantagetcg.com/data-privacy-day-2020-what-is-your-data-net-worth/ (accessed 1.21.21).

Grundy, Q., Held, F.P., Bero, L.A., 2017. Tracing the potential flow of consumer data: A network analysis of prominent health and fitness apps. J. Med. Internet Res. 19. https://doi.org/10.2196/jmir.7347

Gu, J., Xu, Y. (Calvin), Xu, H., Zhang, C., Ling, H., 2017. Privacy concerns for mobile app download: An elaboration likelihood model perspective. Decis. Support Syst. 94, 19–28. https://doi.org/10.1016/j.dss.2016.10.002

Gu, J., Xu, Y., Xu, H., Ling, H., 2015. Interaction Effects of Contextual Cues on Privacy Concerns: the Case of Android Applications, in: Bui, T.X., Sprague, R.H. (Eds.), 2015 48th Hawaii International Conference on System Sciences (Hicss). pp. 3498–3507.

Guba, E., Lincoln, Y., 1994. Competing Paradigms in Qualitative Research, Handbook of qualitative research. Thousand Oaks, CA: Sage.

Guinchard, A., 2020. Our digital footprint under Covid-19: should we fear the UK digital contact tracing app? Int. Rev. Law Comput. Technol. 1–14.

Gustarini, M., Wac, K., Dey, A.K., 2016. Anonymous smartphone data collection: factors influencing the users' acceptance in mobile crowd sensing. Pers. Ubiquitous Comput. 20, 65–82. https://doi.org/10.1007/s00779-015-0898-0

Hallam, C., Zanella, G., 2017. Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. Comput. Hum. Behav. 68, 217–227. https://doi.org/10.1016/j.chb.2016.11.033

Hammersley, M., 1992. The Paradigm Wars: Reports from the Front. Br. J. Sociol. Educ. 13, 131–143.

Hann, I.-H., Hui, K.-L., Lee, S.-Y.T., Png, I.P.L., 2007. Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach. J. Manag. Inf. Syst. 24, 13–42. https://doi.org/10.2753/MIS0742-1222240202

Harari, G.M., Lane, N.D., Wang, R., Crosier, B.S., Campbell, A.T., Gosling, S.D., 2016. Using Smartphones to Collect Behavioral Data in Psychological Science: Opportunities, Practical Considerations, and Challenges. Perspect. Psychol. Sci. 11, 838–854. https://doi.org/10.1177/1745691616650285

Hassan, N.R., Lowry, P.B., 2015. Seeking middle-range theories in information systems research, in: International Conference on Information Systems (ICIS 2015), Fort Worth, TX, December. pp. 13–18.

Hassan, N.R., Mathiassen, L., Lowry, P., 2019a. ENHANCING THEORETICAL CONTRIBUTION IN IS RESEARCH: THE CASE OF TECHNOLOGY ADOPTION 17.

Hassan, N.R., Mathiassen, L., Lowry, P.B., 2019b. The process of information systems theorizing as a discursive practice. J. Inf. Technol. 34, 198–220.

Hatamian, M., Serna, J., Rannenberg, K., 2019. Revealing the unrevealed: Mining smartphone users privacy perception on app markets. Comput. Secur. 83, 332–353. https://doi.org/10.1016/j.cose.2019.02.010

Heath, H., Cowley, S., 2004. Developing a grounded theory approach: a comparison of Glaser and Strauss. Int. J. Nurs. Stud. 41, 141–150. https://doi.org/10.1016/S0020-7489(03)00113-5

Hern, A., Pegg, D., 2018. Facebook fined for data breaches in Cambridge Analytica scandal. The Guardian.

Hinz, Hann, Spann, 2011. Price Discrimination in E-Commerce? An Examination of Dynamic Pricing in Name-Your-Own Price Markets. MIS Q. 35, 81. https://doi.org/10.2307/23043490

Hirschprung, R., Toch, E., Bolton, F., Maimon, O., 2016. A methodology for estimating the value of privacy in information disclosure systems. Comput. Hum. Behav. 61, 443–453. https://doi.org/10.1016/j.chb.2016.03.033

Hodgson, G.M., 2012. On the limits of rational choice theory. Econ. Thought 1.

Hong, W., Chan, F.K.Y., Thong, J.Y.L., 2019. Drivers and Inhibitors of Internet Privacy Concern: A Multidimensional Development Theory Perspective. J. Bus. Ethics. https://doi.org/10.1007/s10551-019-04237-1

Huberman, B.A., Adar, E., Fine, L.R., 2005. Valuating privacy. Secur. Priv. IEEE 3, 22–25.

Huckvale, K., Prieto, J.T., Tilney, M., Benghozi, P.-J., Car, J., 2015. Unaddressed privacy risks in accredited health and wellness apps: A cross-sectional systematic assessment. BMC Med. 13. https://doi.org/10.1186/s12916-015-0444-y

Huebner, J., Girardello, A., Sliz, O., Fleisch, E., Ilic, A., 2020. What People Focus on When Reviewing Your App: An Analysis Across App Categories. IEEE Softw. 0–0. https://doi.org/10.1109/MS.2020.3014669

Hui, K.-L., Tan, B.C.Y., Goh, C.-Y., 2006. Online Information Disclosure: Motivators and Measurements. ACM Trans Internet Technol 6, 415–441. https://doi.org/10.1145/1183463.1183467

Hutchison, A.J., Johnston, L.H., Breckon, J.D., 2010. Using QSR-NVivo to facilitate the development of a grounded theory project: an account of a worked example. Int. J. Soc. Res. Methodol. 13, 283–302. https://doi.org/10.1080/13645570902996301

ICO, 2020. GDPR Principles [WWW Document]. URL https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/ (accessed 11.19.20).

Inayat, I., Salim, S.S., Marczak, S., Daneva, M., Shamshirband, S., 2015. A systematic literature review on agile requirements engineering practices and challenges. Comput. Hum. Behav. 51, 915–929. https://doi.org/10.1016/j.chb.2014.10.046

Jai, T.-M.C., King, N.J., 2016. Privacy versus reward: Do loyalty programs increase consumers' willingness to share personal information with third-party advertisers and data brokers? J. Retail. Consum. Serv. 28, 296–303.

Jalali, S., Wohlin, C., 2012. Systematic literature studies: database searches vs. backward snowballing, in: Proceedings of the ACM-IEEE International Symposium on Empirical Software Engineering and Measurement - ESEM '12. Presented at the the ACM-IEEE international symposium, ACM Press, Lund, Sweden, p. 29. https://doi.org/10.1145/2372251.2372257

Jamshed, S., 2014. Qualitative research method-interviewing and observation. J. Basic Clin. Pharm. 5, 87–88. https://doi.org/10.4103/0976-0105.141942

Jebb, A.T., Parrigon, S., Woo, S.E., 2017. Exploratory data analysis as a foundation of inductive research. Hum. Resour. Manag. Rev. 27, 265–276. https://doi.org/10.1016/j.hrmr.2016.08.003

Jens, R., Grosvold, J., U., H.S., 2014. Reputational risks and sustainable supply chain management: Decision making under bounded rationality. Int. J. Oper. Prod. Manag. 34, 695–719. https://doi.org/10.1108/IJOPM-10-2012-0449

Jensen, K.B., Rothenbuhler, E.W., Pooley, J.D., Craig, R.T. (Eds.), 2016. The International Encyclopedia of Communication Theory and Philosophy, 1st ed. Wiley. https://doi.org/10.1002/9781118766804

Jeong, S.-H., Kim, H., Yum, J.-Y., Hwang, Y., 2016. What type of content are smartphone users addicted to?: SNS vs. games. Comput. Hum. Behav. 54, 10–17. https://doi.org/10.1016/j.chb.2015.07.035

Jibril, A.B., Kwarteng, M.A., Nwaiwu, F., Appiah-Nimo, C., Pilik, M., Chovancova, M., 2020. Online Identity Theft on Consumer Purchase Intention: A Mediating Role of Online Security and Privacy Concern, in: Conference on E-Business, e-Services and e-Society. Springer, pp. 147–158.

John, L.K., Acquisti, A., Loewenstein, G., 2011. Strangers on a plane: Context-dependent willingness to divulge sensitive information. J. Consum. Res. 37, 858–873. https://doi.org/10.1086/656423

Jokinen, J., 2017. Touch Screen Text Entry as Cognitively Bounded Rationality. Cogn. Sci.

Jones, S.L., Ferreira, D., Hosio, S., Goncalves, J., Kostakos, V., 2015. Revisitation analysis of smartphone app use, in: Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing - UbiComp '15. Presented at the the 2015 ACM International Joint Conference, ACM Press, Osaka, Japan, pp. 1197–1208. https://doi.org/10.1145/2750858.2807542

Junglas, I.A., Johnson, N.A., Spitzmüller, C., 2008. Personality traits and concern for privacy: an empirical study in the context of location-based services. Eur. J. Inf. Syst. 17, 387–402. https://doi.org/10.1057/ejis.2008.29

Kaplan, B., Duchon, D., 1988. Combining Qualitative and Quantitative Methods in Information Systems Research: A Case Study. MIS Q. 12, 571–586.

Keith, M.J., Thompson, S.C., Hale, J., Lowry, P.B., Greer, C., 2013. Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. Int. J. Hum.-Comput. Stud. 71, 1163–1173. https://doi.org/10.1016/j.ijhcs.2013.08.016

Ketelaar, P.E., van Balen, M., 2018. The smartphone as your follower: The role of smartphone literacy in the relation between privacy concerns, attitude and behaviour towards phone-embedded tracking. Comput. Hum. Behav. 78, 174–182. https://doi.org/10.1016/j.chb.2017.09.034

Kim, D., Koohikamali, M., 2015. Does Information Sensitivity Make A Difference? Mobile Applications' Privacy Statements: A Text Mining Approach. AMCIS 2015 Proc.

Kim, H.-S., 2016. What drives you to check in on Facebook? Motivations, privacy concerns, and mobile phone involvement for location-based information sharing. Comput. Hum. Behav. 54, 397–406. https://doi.org/10.1016/j.chb.2015.08.016

Klein, H.K., Myers, M.D., 1999. A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems. MIS Q. 23, 67. https://doi.org/10.2307/249410

Knijnenburg, B., Raybourn, E., Cherry, D., Wilkinson, D., Sivakumar, S., Sloan, H., 2017. Death to the Privacy Calculus? Available SSRN 2923806.

Knijnenburg, B.P., 2017. Privacy? I Can't Even! Making a Case for User-Tailored Privacy. IEEE Secur. Priv. 15, 62–67. https://doi.org/10.1109/MSP.2017.3151331

Knijnenburg, B.P., Kobsa, A., 2013. Making decisions about privacy: Information disclosure in context-aware recommender systems. ACM Trans. Interact. Intell. Syst. 3. https://doi.org/10.1145/2499670

Kokkoris, M.D., Kamleitner, B., 2020. Would You Sacrifice Your Privacy to Protect Public Health? Prosocial Responsibility in a Pandemic Paves the Way for Digital Surveillance. Front. Psychol. 11. https://doi.org/10.3389/fpsyg.2020.578618

Kokolakis, S., 2015. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Comput. Secur. https://doi.org/10.1016/j.cose.2015.07.002

Koohikamali, M., Gerhart, N., Mousavizadeh, M., 2015. Location disclosure on LB-SNAs: The role of incentives on sharing behavior. Decis. Support Syst. 71, 78–87. https://doi.org/10.1016/j.dss.2015.01.008

Köping, L., Shirahama, K., Grzegorzek, M., 2018. A general framework for sensor-based human activity recognition. Comput. Biol. Med. 95, 248–260. https://doi.org/10.1016/j.compbiomed.2017.12.025

Korpilo, S., Virtanen, T., Lehvävirta, S., 2017. Smartphone GPS tracking—Inexpensive and efficient data collection on recreational movement. Landsc. Urban Plan. 157, 608–617. https://doi.org/10.1016/j.landurbplan.2016.08.005

Kostakos, V., Venkatanathan, J., Reynolds, B., Sadeh, N., Toch, E., Shaikh, S.A., Jones, S., 2011. Who's your best friend?: targeted privacy attacks In location-sharing social networks. ACM Press, p. 177. https://doi.org/10.1145/2030112.2030138

Kulyk, O., Gerber, P., Marky, K., Beckmann, C., Volkamer, M., 2019. Does This App Respect My Privacy? Design and Evaluation of Information Materials Supporting Privacy-Related Decisions of Smartphone Users, in: Proceedings 2019 Workshop on Usable Security. Presented at the Workshop on Usable Security, Internet Society, San Diego, CA. https://doi.org/10.14722/usec.2019.23029

Kumaraguru, P., Cranor, L.F., 2005. Privacy Indexes: A Survey of Westin's Studies (Academic No. CMU-ISRI-5-138). Institute for Software Research International School of Computer Science, Carnegie Mellon University.

Kusyanti, A., Puspa, H., 2018. An Empirical Study of App Permissions : A User Protection Motivation Behaviour. Int. J. Adv. Comput. Sci. Appl. 9. https://doi.org/10.14569/IJACSA.2018.091116

Lee, H., Lim, D., Kim, H., Zo, H., Ciganek, A.P., 2015. Compensation paradox: the influence of monetary rewards on user behaviour. Behav. Inf. Technol. 34, 45–56. https://doi.org/10.1080/0144929X.2013.805244

Lee, H., Park, H., Kim, J., 2013. Why do people share their context information on Social Network Services? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk. Int. J. Hum.-Comput. Stud. 71, 862–877. https://doi.org/10.1016/j.ijhcs.2013.01.005

Leith, D.J., Farrell, S., 2020. Gaen due diligence: Verifying the Google/Apple COVID exposure notification API. CoronaDef21 Proc. NDSS '21 2021.

Li, H., Lu, X., Liu, X., Xie, T., Bian, K., Lin, F.X., Mei, Q., Feng, F., 2015. Characterizing Smartphone Usage Patterns from Millions of Android Users, in: Proceedings of the 2015 ACM Conference on Internet Measurement Conference - IMC '15. Presented at the the 2015 ACM Conference, ACM Press, Tokyo, Japan, pp. 459–472. https://doi.org/10.1145/2815675.2815686

Li, H., Sarathy, R., Xu, H., 2010. Understanding Situational Online Information Disclosure as a Privacy Calculus. J. Comput. Inf. Syst. Stillwater 51, 62–71.

Li, K., Wang, X., Li, K., Che, J., 2016. Information privacy disclosure on social network sites: An empirical investigation from social exchange perspective. Nankai Bus. Rev. Int. 7, 282–300. https://doi.org/10.1108/NBRI-02-2015-0005

Li, Y., 2012. Theories in online information privacy research: A critical review and an integrated framework. Decis. Support Syst. 54, 471–481. https://doi.org/10.1016/j.dss.2012.06.010

Lin, I.-C., Lin, Y.-W., Wu, Y.-S., 2016. Corresponding Security Level with the Risk Factors of Personally Identifiable Information through the Analytic Hierarchy Process. J. Comput. 11, 124–131.

Lindorff, M., 2010. Ethics, ethical human research and human research ethics committees. Aust. Univ. Rev. 52, 51–59.

Liu, B., Andersen, M.S., Schaub, F., Almuhimedi, H., Zhang, S. (Aerin), Sadeh, N., Agarwal, Y., Acquisti, A., 2016. Follow My Recommendations: A Personalized Privacy Assistant for Mobile App Permissions, in: Twelfth Symposium on Usable Privacy and Security (SOUPS 2016). USENIX Association, Denver, CO, pp. 27–41.

Liu, N., Yu, R., 2017. Identifying design feature factors critical to acceptance and usage behavior of smartphones. Comput. Hum. Behav. 70, 131–142. https://doi.org/10.1016/j.chb.2016.12.073

Locke, K., 1996. Rewriting the Discovery of Grounded Theory after 25 Years? J. Manag. Inq. 5, 239–245. https://doi.org/10.1177/105649269653008

Lwin, M., Wirtz, J., Williams, J.D., 2007. Consumer online privacy concerns and responses: a power–responsibility equilibrium perspective. J. Acad. Mark. Sci. 35, 572–585. https://doi.org/10.1007/s11747-006-0003-3

Magsamen-Conrad, K., 2014. Dimensions of anticipated reaction in information management: Anticipating responses and outcomes. Rev. Commun. 14, 314–333. https://doi.org/10.1080/15358593.2014.986514

Malheiros, M., Preibusch, S., Sasse, M.A., 2013. “Fairly Truthful”: The Impact of Perceived Effort, Fairness, Relevance, and Sensitivity on Personal Data Disclosure, in: Trust and Trustworthy Computing. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 250–266.

Malhotra, N.K., Kim, S.S., Agarwal, J., 2004. Internet Users’ Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. Inf. Syst. Res. 15, 336–355. https://doi.org/10.1287/isre.1040.0032

Malmqvist, J., Hellberg, K., Möll\aas, G., Rose, R., Shevlin, M., 2019. Conducting the pilot study: A neglected part of the research process? Methodological findings supporting the importance of piloting in qualitative research studies. Int. J. Qual. Methods 18, 1609406919878341.

March, J.G., 1978. Bounded Rationality, Ambiguity, and the Engineering of Choice. Bell J. Econ. 9, 587. https://doi.org/10.2307/3003600

Markos, E., Labrecque, L.I., Milne, G.R., 2018. A New Information Lens: The Self-concept and Exchange Context as a Means to Understand Information Sensitivity of Anonymous and Personal Identifying Information. J. Interact. Mark. 42, 46–62. https://doi.org/10.1016/j.intmar.2018.01.004

Markos, E., Milne, G.R., Peltier, J.W., 2017. Information Sensitivity and Willingness to Provide Continua: A Comparative Privacy Study of the United States and Brazil. J. Public Policy Mark. 36, 79–96. https://doi.org/10.1509/jppm.15.159

Martin, G., Gupta, H., Wingreen, S.C., Mills, A., 2016. An Analysis of Personal Information Privacy Concerns Using Q-Methodology. ArXiv abs/1606.03547.

Martin-Consuegra, D., Gomez, M., Molina, A., 2015. Consumer Sensitivity Analysis in Mobile Commerce Advertising. Soc. Behav. Personal. 43, 883–898. https://doi.org/10.2224/sbp.2015.43.6.883

Martinez-Balleste, A., Perez-martinez, P., Solanas, A., 2013. The pursuit of citizens’ privacy: a privacy-aware smart city is possible. IEEE Commun. Mag. 51, 136–141. https://doi.org/10.1109/MCOM.2013.6525606

Martínez-Pérez, B., de la Torre-Díez, I., López-Coronado, M., 2015. Privacy and Security in Mobile Health Apps: A Review and Recommendations. J. Med. Syst. 39, 181. https://doi.org/10.1007/s10916-014-0181-3

Mason, J., 2002. Analyzing Qualitative Data. Routledge.

Mekovec, R., Hrustek, N.Ž., Pihir, I., 2017. On-Line Behaviour of Users With Different Privacy Concerns 6.

Michael, K., Clarke, R., 2013. Location and tracking of mobile devices: Überveillance stalks the streets. Comput. Law Secur. Rev. 29, 216–228. https://doi.org/10.1016/j.clsr.2013.03.004

Michael, M., Michael, K., 2010. Toward a State of Überveillance [Special Section Introduction. IEEE Technol. Soc. Mag. 29, 9–16. https://doi.org/10.1109/MTS.2010.937024

Miller, A.R., 1972. Review of The Assault on Privacy: Computers, Data Banks, and Dossiers. Am. Arch. 35, 403–405.

Milne, G.R., Bahl, S., 2010. Are There Differences between Consumers' and Marketers' Privacy Expectations? A Segment- and Technology-Level Analysis. J. Public Policy Mark. 29, 138–149. https://doi.org/10.1509/jppm.29.1.138

Milne, G.R., Culnan, M.J., 2004. Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. J. Interact. Mark. 18, 15–29. https://doi.org/10.1002/dir.20009

Milne, G.R., Pettinico, G., Hajjat, F.M., Markos, E., 2017. Information Sensitivity Typology: Mapping the Degree and Type of Risk Consumers Perceive in Personal Data Sharing. J. Consum. Aff. 51, 133–161. https://doi.org/10.1111/joca.12111

Morton, A., Sasse, M.A., 2014. Desperately seeking assurances: Segmenting users by their information-seeking preferences. Presented at the 2014 12th Annual Conference on Privacy, Security and Trust, PST 2014, pp. 102–111. https://doi.org/10.1109/PST.2014.6890929

Mothersbaugh, D.L., Foxx, W.K., Beatty, S.E., Wang, S., 2012. Disclosure Antecedents in an Online Service Context: The Role of Sensitivity of Information. J. Serv. Res. 15, 76–98. https://doi.org/10.1177/1094670511424924

Mousavi, R., Chen, R., Kim, D.J., Chen, K., 2020. Effectiveness of privacy assurance mechanisms in users' privacy protection on social networking sites from the perspective of protection motivation theory. Decis. Support Syst. 135, 113323. https://doi.org/10.1016/j.dss.2020.113323

Myers, M.D., 2009. Qualitative research in business and management. SAGE, Los Angeles.

Myers, M.D., Avison, D.E. (Eds.), 2002. Qualitative research in information systems: a reader, Introducing qualitative methods. SAGE, London ; Thousand Oaks, Calif.

Ndibwile, J.D., Luhanga, E.T., Fall, D., Miyamoto, D., Kadobayashi, Y., 2018. A comparative study of smartphone-user security perception and preference towards redesigned security notifications, in: Proceedings of the Second African Conference for Human Computer Interaction on Thriving Communities - AfriCHI '18. Presented at the the Second African Conference for Human Computer Interaction, ACM Press, Windhoek, Namibia, pp. 1–6. https://doi.org/10.1145/3283458.3283486

Nissenbaum, H., 2004. Privacy as contextual integrity. Wash Rev 79, 119.

Noain-Sánchez, A., 2016. "Privacy by default" and active "informed consent" by layers: Essential measures to protect ICT users' privacy. J. Inf. Commun. Ethics Soc. 14, 124–138. https://doi.org/10.1108/JICES-10-2014-0040

Oates, B.J., 2006. Researching information systems and computing. SAGE Publications, London ; Thousand Oaks, Calif.

Ofcom, 2018. Communications Market Report.

Office for National Statistics, 2019. Overview of the UK population - Office for National Statistics [WWW Document]. Overv. UK Popul. August 2019. URL https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationestimates/articles/overviewoftheukpopulation/august2019#main-points (accessed 12.21.20).

Office for National Statistics, 2017. Household disposable income and inequality in the UK - Office for National Statistics [WWW Document]. URL https://www.ons.gov.uk/peoplepopulationandcommunity/personalandhouseholdfinances/incomeandwealth/bulletins/householddisposableincomeandinequality/financialyearending2016

Okamoto, T., Yatsuhashi, J., Mizutani, N., 2017. University Students' Priorities for Smartphone Applications in Online Purchasing, in: Proceedings of the 4th Multidisciplinary International Social Networks Conference on ZZZ - MISNC '17. Presented at the the 4th Multidisciplinary International Social Networks Conference, ACM Press, Bangkok, Thailand, pp. 1–6. https://doi.org/10.1145/3092090.3092101

Oliveira, A., 2007. A Discussion of Rational and Psychological Decision-Making Theories and Models: The Search for a Cultural-Ethical Decision-Making Model 12, 6.

Olmstead, K., Atkinson, M., 2015. Apps Permissions in the Google Play Store. Pew Res. Cent. Internet Sci. Tech. URL http://www.pewinternet.org/2015/11/10/apps-permissions-in-the-google-play-store/ (accessed 11.24.17).

Olukoya, O., Mackenzie, L., Omoronyia, I., 2020. Security-oriented view of app behaviour using textual descriptions and user-granted permission requests. Comput. Secur. 89, 101685. https://doi.org/10.1016/j.cose.2019.101685

O'Reilly-Shah, V.N., 2017. Factors influencing healthcare provider respondent fatigue answering a globally administered in-app survey. PeerJ 2017. https://doi.org/10.7717/peerj.3785

Orlikowski, W.J., Baroudi, J.J., 1991. Studying Information Technology in Organizations: Research Approaches and Assumptions. Inf. Syst. Res. 2, 1–28.

Osanloo, A., Grant, C., 2016. Understanding, selecting, and integrating a theoretical framework in dissertation research: Creating the blueprint for your "house." Adm. Issues J. Connect. Educ. Pract. Res. 4, 7.

Osatuyi, B., Passerini, K., Ravarini, A., Grandhi, S.A., 2018. " Fool me once, shame on you … then, I learn." An examination of information disclosure in social networking sites. Comput. Hum. Behav. 83, 73–86. https://doi.org/10.1016/j.chb.2018.01.018

Owen, S., 2001. The practical, methodological and ethical dilemmas of conducting focus groups with vulnerable clients. J. Adv. Nurs. 36, 652–658.

Page, S.A., Nyeboer, J., 2017. Improving the process of research ethics review. Res. Integr. Peer Rev. 2, 1–7.

Paine, C., Reips, U.-D., Stieger, S., Joinson, A., Buchanan, T., 2007. Internet users' perceptions of 'privacy concerns' and 'privacy actions. Int. J. Hum. - Comput. Stud. 65, 526–536. https://doi.org/10.1016/j.ijhcs.2006.12.001

Palinkas, L.A., Horwitz, S.M., Green, C.A., Wisdom, J.P., Duan, N., Hoagwood, K., 2015. Purposeful Sampling for Qualitative Data Collection and Analysis in Mixed Method Implementation Research. Adm. Policy Ment. Health Ment. Health Serv. Res. 42, 533–544. https://doi.org/10.1007/s10488-013-0528-y

Panichas, G.E., 2014. An Intrusion Theory of Privacy. Res Publica 20, 145–161. https://doi.org/10.1007/s11158-014-9240-3

Park, M., Oh, H., Lee, K., 2019. Security Risk Measurement for Information Leakage in IoT-Based Smart Homes from a Situational Awareness Perspective. Sensors 19, 2148. https://doi.org/10.3390/s19092148

Patriana Ch, R., Irawan, I., Tampubolon, S., Pane, M.M., 2015. Benefits of using smartphones for improving students' learning outcomes at BINUS University. Adv. Sci. Lett. 21, 2396–2399. https://doi.org/10.1166/asl.2015.6288

Pavlou, P.A., 2011. State of the Information Privacy Literature: Where Are We Now and Where Should We Go? MIS Q 35, 977–988.

Pennekamp, J., Henze, M., Wehrle, K., 2017. A survey on the evolution of privacy enforcement on smartphones and the road ahead. Pervasive Mob. Comput. 42, 58–76. https://doi.org/10.1016/j.pmcj.2017.09.005

Petronio, S.S., 2002. Boundaries of privacy: dialectics of disclosure, SUNY series in communication studies. State University of New York Press, Albany.

Pournajaf, L., Garcia-Ulloa, D.A., Xiong, L., Sunderam, V., 2015. Participant privacy in mobile crowd sensing task management: A survey of methods and challenges. SIGMOD Rec. 44, 23–34. https://doi.org/10.1145/2935694.2935700

Preibusch, S., 2013. Guide to measuring privacy concern: Review of survey and observational instruments. Int. J. Hum.-Comput. Stud. 71, 1133–1143. https://doi.org/10.1016/j.ijhcs.2013.09.002

Rahi, S., 2017. Research Design and Methods: A Systematic Review of Research Paradigms, Sampling Issues and Instruments Development. Int. J. Econ. Manag. Sci. 06. https://doi.org/10.4172/2162-6359.1000403

Rahmati, A., Tossell, C., Shepard, C., Kortum, P., Zhong, L., 2012. Exploring iPhone usage: the influence of socioeconomic differences on smartphone adoption, usage and usability, in: Proceedings of the 14th International Conference on Human-Computer Interaction with Mobile Devices and Services - MobileHCI '12. Presented at the the 14th international conference, ACM Press, San Francisco, California, USA, p. 11. https://doi.org/10.1145/2371574.2371577

Rapley, T., Rees, G., 2018. Collecting Documents as Data, in: The SAGE Handbook of Qualitative Data Collection. SAGE Publications Ltd, 1 Oliver's Yard, 55 City Road, London EC1Y 1SP, pp. 378–391. https://doi.org/10.4135/9781526416070.n24

Rashidi, B., Fung, C., Vu, T., 2016. Android fine-grained permission control system with real-time expert recommendations. Pervasive Mob. Comput. 32, 62–77. https://doi.org/10.1016/j.pmcj.2016.04.013

Rastogi, S., Bhushan, K., Gupta, B.B., 2016. Android Applications Repackaging Detection Techniques for Smartphone Devices. Procedia Comput. Sci. 78, 26–32. https://doi.org/10.1016/j.procs.2016.02.006

Recker, J., 2013. Scientific research in information systems: a beginner's guide, Progress in IS. Springer, Berlin Heidelberg New York Dobrecht London.

Rendina, H.J., Mustanski, B., 2018. Privacy, Trust, and Data Sharing in Web-Based and Mobile Research: Participant Perspectives in a Large Nationwide Sample of Men Who Have Sex With Men in the United States. J. Med. Internet Res. 20, e233. https://doi.org/10.2196/jmir.9019

Ritchie, J., Lewis, J., McNaughton Nicholls, C., Ormston, R. (Eds.), 2014. Qualitative research practice: a guide for social science students and researchers, Second edition. ed. Sage, Los Angeles.

Rochelandet, F., Acquisti, A., 2011. Privacy in electronic commerce and the economics of immediate gratification. Réseaux 167, 105–130. https://doi.org/10.3917/res.167.0105

Rose, C., 2012. Ubiquitous Smartphones, Zero Privacy. Rev. Bus. Inf. Syst. Online Littleton 16, 187.

Rosen, M., 1991. COMING TO TERMS WITH THE FIELD: UNDERSTANDING AND DOING ORGANIZATIONAL ETHNOGRAPHY*. J. Manag. Stud. 28, 1–24. https://doi.org/10.1111/j.1467-6486.1991.tb00268.x

RSA, 2019. RSA Data Privacy & Security Survey 2019 16.

Rubinstein, A., 1998. Modeling bounded rationality. MIT press.

Schaub, F., Balebako, R., Cranor, L.F., 2017. Designing effective privacy notices and controls. IEEE Internet Comput.

Schudy, S., Utikal, V., 2017. 'You must not know about me'—On the willingness to share personal data. J. Econ. Behav. Organ. 141, 1–13. https://doi.org/10.1016/j.jebo.2017.05.023

Schwartz, P., Solove, D.J., 2011. The PII Problem: Privacy and New Concept of Personally Identifiable Information. N. Y. Univ. Law Rev. 86, 1814–1894.

Seawright, J., Gerring, J., 2008. Case selection techniques in case study research: A menu of qualitative and quantitative options. Polit. Res. Q. 61, 294–308.

Semanjski, I., Gautama, S., 2016. Crowdsourcing mobility insights – Reflection of attitude based segments on high resolution mobility behaviour data. Transp. Res. Part C Emerg. Technol. 71, 434–446. https://doi.org/10.1016/j.trc.2016.08.016

Sheehy-Skeffington, J., Rea, J., 2017. How poverty affects people's decision-making processes (SSRN Scholarly Paper). LSE, London, UNITED KINGDOM.

Shih, F., Liccardi, I., Weitzner, D., 2015. Privacy Tipping Points in Smartphones Privacy Preferences, in: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, CHI '15. ACM, New York, NY, USA, pp. 807–816. https://doi.org/10.1145/2702123.2702404

Shklovski, I., Mainwaring, S.D., Skúladóttir, H.H., Borgthorsson, H., 2014. Leakiness and creepiness in app space: perceptions of privacy and mobile app use. ACM Press, pp. 2347–2356. https://doi.org/10.1145/2556288.2557421

Sikolia, D., Biros, D., Mason, M., Weiser, M., 2013. Trustworthiness of Grounded Theory Methodology Research in Information Systems. MWAIS 2013 Proceedings. 16.https://aisel.aisnet.org/mwais2013/16

Silverman, D., 1998. Qualitative research: meanings or practices? Inf. Syst. J. 8, 3–20. https://doi.org/10.1046/j.1365-2575.1998.00002.x

Simmel, A., 2007. Privacy is not an Isolated Freedom, in: Privacy & Personality. Aldine Transaction, New Brunswick (U.S.A.).

Simon, H.A., 1982. Models of bounded rationality. MIT Press, Cambridge, Mass.

Sipior, J.C., Ward, B.T., Volonino, L., 2014. Privacy Concerns Associated with Smartphone Use. J. Internet Commer. 13, 177–193. https://doi.org/10.1080/15332861.2014.947902

Smith, H., Dinev, T., Xu, H., 2011. Information Privacy Research: An Interdisciplinary Review. Manag. Inf. Syst. Q. 35, 989–1015.

Smith, H.J., Dinev, T., Xu, H., 2011. INFORMATION PRIVACY RESEARCH: AN INTERDISCIPLINARY REVIEW. MIS Quarterly Vol. 35, 989–1015.

Smith, H.J., Milberg, S.J., Burke, S.J., 1996. Information Privacy: Measuring Individuals' Concerns About Organizational Practices. MIS Q. 20, 167–196.

Solove, D.J., 2003. Identity Theft, Privacy, and the Architecture of Vulnerability (SSRN Scholarly Paper No. ID 416740). Social Science Research Network, Rochester, NY.

Solove, D.J., 2002. Conceptualizing Privacy. Calif. Law Rev. 90, 1087. https://doi.org/10.2307/3481326

Son, J.-Y., Kim, S.S., 2008. Internet users' information privacy-protective responses: A Taxonomy and a nomological model. MIS Q. Manag. Inf. Syst. 32, 503–529.

Spiegel, T., Silva, A.C.P.V., 2018. Decision-Making Cognitive Process: Let's not Forget That Healthcare Professionals are Human. Int. J. Comput. Clin. Pract. 3, 1–12. https://doi.org/10.4018/IJCCP.2018010101

Spiekermann, S., Acquisti, A., Böhme, R., Hui, K.-L., 2015. The challenges of personal data markets and privacy. Electron. Mark. 25, 161–167. https://doi.org/10.1007/s12525-015-0191-0

Stahl, B.C., Wright, D., 2018. Proactive Engagement with Ethics and Privacy in AI and Big Data - Implementing responsible research and innovation in AI-related projects.

Strauss, A.L., Corbin, J.M., 1998. Basics of qualitative research: techniques and procedures for developing grounded theory. Sage Publications, Thousand Oaks.

Strickland, L.S., Hunt, L.E., 2005. Technology, security, and individual privacy: New tools, new threats, and new public perceptions. J. Am. Soc. Inf. Sci. Technol. 56, 221–234. https://doi.org/10.1002/asi.20122

Stuart, A., Bandara, A.K., Levine, M., 2019. The psychology of privacy in the digital age. Soc. Personal. Psychol. Compass 13. https://doi.org/10.1111/spc3.12507

Surma, D.R., Geise, M.J., Lehman, J., Beasley, R., Palmer, K., 2012. Computer Literacy: What It Means and Do Today's College Students Need a Formal Course in It? J Comput Sci Coll 28, 142–143.

Taneja, A., Vitrano, J., Gengo, N.J., 2014. Rationality-based beliefs affecting individual's attitude and intention to use privacy controls on Facebook: An empirical

investigation. Comput. Hum. Behav. 38, 159–173. https://doi.org/10.1016/j.chb.2014.05.027

Tavani, H., 2008. Informational Privacy: Concepts, Theories, and Controversies, in: AND COMPUTER ETHICS THE HANDBOOK OF INFORMATION AND COMPUTER ETHICS Edited By. Wiley, Hoboken, New Jersey, pp. 166–706.

Tavani, H., 2007. PHILOSOPHICAL THEORIES OF PRIVACY: IMPLICATIONS FOR AN ADEQUATE ONLINE PRIVACY POLICY. Metaphilosophy 38, 1–22. https://doi.org/10.1111/j.1467-9973.2006.00474.x

Tavani, H.T., 2007. Philosophical theories of privacy: Implications for an adequate online privacy policy. Metaphilosophy 38, 1–22.

Tavani, H.T., Moor, J.H., 2001. Privacy protection, control of information, and privacy-enhancing technologies. ACM SIGCAS Comput. Soc. 31, 6–11. https://doi.org/10.1145/572277.572278

Taylor, V.F., Martinovic, I., 2016. SecuRank: Starving Permission-Hungry Apps Using Contextual Permission Analysis, in: Proceedings of the 6th Workshop on Security and Privacy in Smartphones and Mobile Devices - SPSM'16. Presented at the the 6th Workshop, ACM Press, Vienna, Austria, pp. 43–52. https://doi.org/10.1145/2994459.2994474

Technology, T., 2017. Location tracking | Me and my Shadow [WWW Document]. URL https://myshadow.org/ (accessed 12.9.17).

Thomas, L., Little, L., Briggs, P., McInnes, L., Jones, E., Nicholson, J., 2013. Location tracking: views from the older adult population. Age Ageing 42, 758–763. https://doi.org/10.1093/ageing/aft069

Thory, K., 2016. To Reveal or Conceal? Managers' Disclosures of Private Information During Emotional Intelligence Training. Hum. Resour. Dev. Q. 27, 41–66. https://doi.org/10.1002/hrdq.21222

Timonen, V., Foley, G., Conlon, C., 2018. Challenges When Using Grounded Theory: A Pragmatic Introduction to Doing GT Research. Int. J. Qual. Methods 17, 160940691875808. https://doi.org/10.1177/1609406918758086

Tsui, A., 2016. Reflections on the so-called value-free ideal. Cross Cult. Strateg. Manag.

Turner, D., 2010. Qualitative Interview Design: A Practical Guide for Novice Investigators. Qual. Rep. 15, 754–760.

Turow, J., Hennessy, M., Bleakley, A., 2008. Consumers' understanding of privacy rules in the marketplace. J. Consum. Aff. 42, 411–424.

Turow, J., King, J., Hoofnagle, C.J., Bleakley, A., Hennessy, M., 2009. Americans Reject Tailored Advertising and Three Activities that Enable It. SSRN Electron. J. https://doi.org/10.2139/ssrn.1478214

UK Government, 2017. A safe and secure cyberspace - making the UK the safest place in the world to live and work online - GOV.UK [WWW Document]. URL https://www.gov.uk/government/publications/uk-digital-strategy/5-a-safe-and-secure-cyberspace-making-the-uk-the-safest-place-in-the-world-to-live-and-work-online.

Urban, J.M., Hoofnagle, C.J., 2014. The privacy pragmatic as privacy vulnerable, in: Symposium on Usable Privacy and Security (SOUPS 2014) Workshop on Privacy Personas and Segmentation (PPS).

Urquhart, C., Lehmann, H., Myers, M.D., 2009. Putting the 'theory' back into grounded theory: guidelines for grounded theory studies in information systems: Guidelines for grounded theory studies in information systems. Inf. Syst. J. 20, 357–381. https://doi.org/10.1111/j.1365-2575.2009.00328.x

Van Heerde, H.J., Dinner, I.M., Neslin, S.A., 2019. Engaging the unengaged customer: The value of a retailer mobile app. Int. J. Res. Mark. 36, 420–438.

Van Wassenhove, W., Dressel, K., Perazzini, A., Ru, G., 2012. A comparative study of stakeholder risk perception and risk communication in Europe: a bovine spongiform encephalopathy case study. J. Risk Res. 15, 565–582. https://doi.org/10.1080/13669877.2011.646290

Vasalou, A., Joinson, A., Houghton, D., 2015. Privacy as a fuzzy concept: A new conceptualization of privacy for practitioners: Privacy as a Fuzzy Concept: A New Conceptualization of Privacy for Practitioners. J. Assoc. Inf. Sci. Technol. 66, 918–929. https://doi.org/10.1002/asi.23220

Venkatesh, V., Brown, S., Bala, H., 2013. Bridging the Qualitative–Quantitative Divide: Guidelines for Conducting Mixed Methods Research in Information Systems. Manag. Inf. Syst. Q. 37, 21–54.

Vogel, S., Draper-Rodi, J., 2017. The importance of pilot studies, how to write them and what they mean. Int. J. Osteopath. Med. 23, 2–3.

Wachter, S., 2018. Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR. Comput. Law Secur. Rev. 34, 436–449. https://doi.org/10.1016/j.clsr.2018.02.002

Wagner, I., He, Y., Rosenberg, D., Janicke, H., 2016. User Interface Design for Privacy Awareness in eHealth Technologies.pdf, in: Proceedings of 13th IEEE Annual Consumer Communications & Networking Conference (CCNC 2016), Las Vegas, USA, January 2016. Presented at the 1st International Workshop on Ambient Assisted Living and eHealth (AALEH 2016), Las Vegas USA.

Walsham, G., 1995. The Emergence of Interpretivism in IS Research. Inf. Syst. Res. 6, 376–394. https://doi.org/10.1287/isre.6.4.376

Wang, H., Calabrese, F., Di Lorenzo, G., Ratti, C., 2010. Transportation mode inference from anonymized and aggregated mobile phone call detail records. IEEE, pp. 318–323. https://doi.org/10.1109/ITSC.2010.5625188

Wang, H., Li, Y., Guo, Y., Agarwal, Y., Hong, J.I., 2017. Understanding the Purpose of Permission Use in Mobile Apps. ACM Trans. Inf. Syst. 35, 43:1-43:40. https://doi.org/10.1145/3086677

Wang, J., Yazdanmehr, A., Li, Y., Rao, H.R., 2017. Opting for Identity Theft Protection Services: The Role of Anticipated Distress.

Wang, P., Hunter, T., Bayen, A.M., Schechtner, K., González, M.C., 2012. Understanding Road Usage Patterns in Urban Areas. Sci. Rep. 2. https://doi.org/10.1038/srep01001

Wang, T., Duong, T.D., Chen, C.C., 2016. Intention to disclose personal information via mobile applications: A privacy calculus perspective. Int. J. Inf. Manag. 36, 531–542. https://doi.org/10.1016/j.ijinfomgt.2016.03.003

Wang, Y., Jia, X., Jin, Q., Ma, J., 2016. Mobile crowdsourcing: Framework, challenges, and solutions. Concurr. Comput. Pract. Exp. 29, n/a-n/a. https://doi.org/10.1002/cpe.3789

Warren, Brandeis, 1890. The Right to Privacy [WWW Document]. URL http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.

Welke, P., Andone, I., Blaszkiewicz, K., Markowetz, A., 2016. Differentiating smartphone users by app usage, in: Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing. Presented at the UbiComp '16: The 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing, ACM, Heidelberg Germany, pp. 519–523. https://doi.org/10.1145/2971648.2971707

Wenz, A., Jäckle, A., Couper, M.P., 2019. Willingness to use mobile technologies for data collection in a probability household panel. Surv. Res. Methods Vol 13, No 1 (2019)-. https://doi.org/10.18148/srm/2019.v1i1.7298

Westin, A.F., 1970. Privacy and freedom. Bodley Head, London.

Wilson, D.W., Valacich, J.S., 2012. Unpacking the privacy paradox: Irrational decision-making within the privacy calculus. Presented at the International Conference on Information Systems, ICIS 2012, pp. 4152–4162.

Wilson, T.P., 1970. Conceptions of interaction and forms of sociological explanation. Am. Sociol. Rev. 697–710.

Wind, D.K., Sapiezynski, P., Furman, M.A., Lehmann, S., 2016. Inferring Stop-Locations from WiFi. PLOS ONE 11, e0149105. https://doi.org/10.1371/journal.pone.0149105

Wisniewski, P.J., Knijnenburg, B.P., Lipford, H.R., 2017. Making privacy personal: Profiling social network users to inform privacy education and nudging. Int. J. Hum.-Comput. Stud. 98, 95–108. https://doi.org/10.1016/j.ijhcs.2016.09.006

Wolfswinkel, J.F., Furtmueller, E., Wilderom, C.P.M., 2013. Using grounded theory as a method for rigorously reviewing literature. Eur. J. Inf. Syst. Basingstoke 22, 45–55. http://dx.doi.org.proxy.library.dmu.ac.uk/10.1057/ejis.2011.51

Woo, S.E., O'Boyle, E.H., Spector, P.E., 2017. Best practices in developing, conducting, and evaluating inductive research. Hum. Resour. Manag. Rev. 27, 255–264. https://doi.org/10.1016/j.hrmr.2016.08.004

Woods, M., Paulus, T., Atkins, D.P., Macklin, R., 2016. Advancing Qualitative Research Using Qualitative Data Analysis Software (QDAS)? Reviewing Potential Versus Practice in Published Studies using ATLAS.ti and NVivo, 1994–2013. Soc. Sci. Comput. Rev. 34, 597–617. https://doi.org/10.1177/0894439315596311

Wu, X., Brown, K.N., Sreenan, C.J., 2013. Analysis of smartphone user mobility traces for opportunistic data collection in wireless sensor networks. Pervasive Mob. Comput. 9, 881–891. https://doi.org/10.1016/j.pmcj.2013.07.003

Wünderlich, V.N., 2010. Qualitative Exploratory Interview Study, in: Wünderlich, V.N. (Ed.), Acceptance of Remote Services: Perception, Adoption, and Continued Usage in Organizational Settings. Gabler, Wiesbaden, pp. 93–130.

Xiao, L., Lu, Q., Guo, F., 2020. Mobile Personalized Recommendation Model based on Privacy Concerns and Context Analysis for the Sustainable Development of M-commerce. Sustainability 12, 3036.

Xu, H., Dinev, T., Smith, J., Hart, P., 2011a. Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances. J. Assoc. Inf. Syst. 12, 798–824.

Yang, H., Sun, D., Liu, C., 2016. Privacy protection of location-based services in mobile big data environments. Int. J. Wirel. Mob. Comput. 11, 10. https://doi.org/10.1504/IJWMC.2016.079458

Yang, Q., Gasti, P., Zhou, G., Farajidavar, A., Balagani, K.S., 2017. On Inferring Browsing Activity on Smartphones via USB Power Analysis Side-Channel. IEEE Trans. Inf. Forensics Secur. 12, 1056–1066. https://doi.org/10.1109/TIFS.2016.2639446

Yasaka, T.M., Lehrich, B.M., Sahyouni, R., 2020. Peer-to-Peer contact tracing: development of a privacy-preserving smartphone app. JMIR MHealth UHealth 8, e18936.

Yin, F.-S., Liu, M.-L., Lin, C.-P., 2015. Forecasting the continuance intention of social networking sites: Assessing privacy risk and usefulness of technology. Technol. Forecast. Soc. Change 99, 267–272. https://doi.org/10.1016/j.techfore.2015.07.019

Yin, R.K., 2014. Case study research: design and methods, Fifth edition. ed. SAGE, Los Angeles.

Young, A.L., Quan-Haase, A., 2013. PRIVACY PROTECTION STRATEGIES ON FACEBOOK: The Internet privacy paradox revisited. Inf. Commun. Soc. 16, 479–500. https://doi.org/10.1080/1369118X.2013.777757

Zaeem, R.N., Manoharan, M., Yang, Y., Barber, K.S., 2017. Modeling and analysis of identity threat behaviors through text mining of identity theft stories. Comput. Secur. 65, 50–63.

Zhang, J., Calabrese, C., Ding, J., Liu, M., Zhang, B., 2018. Advantages and challenges in using mobile apps for field experiments: A systematic review and a case study. Mob. Media Commun. 6, 179–196. https://doi.org/10.1177/2050157917725550

Zhang, T., Rau, P.-L.P., Salvendy, G., 2010. Exploring critical usability factors for handsets. Behav. Inf. Technol. 29, 45–55.

Zhao, S., Pan, G., Zhao, Y., Tao, J., Chen, J., Li, S., Wu, Z., 2017. Mining User Attributes Using Large-Scale APP Lists of Smartphones. IEEE Syst. J. 11, 315–323. https://doi.org/10.1109/JSYST.2015.2431323

Zhao, S., Ramos, J., Tao, J., Jiang, Z., Li, S., Wu, Z., Pan, G., Dey, A.K., 2016. Discovering different kinds of smartphone users through their application usage behaviors, in: Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing - UbiComp '16. Presented at the the 2016 ACM International Joint Conference, ACM Press, Heidelberg, Germany, pp. 498–509. https://doi.org/10.1145/2971648.2971696

Zhou, Y., Piekarska, M., Raake, A., Xu, T., Wu, X., Dong, B., 2017. Control yourself: on user control of privacy settings using personalization and privacy panel on smartphones. Procedia Comput. Sci., 8th International Conference on Ambient Systems, Networks and Technologies, ANT-2017 and the 7th International Conference on Sustainable Energy Information Technology, SEIT 2017, 16-19 May 2017, Madeira, Portugal 109, 100–107. https://doi.org/10.1016/j.procs.2017.05.300

Zhuo, G., Jia, Q., Guo, L., Li, M., Li, P., 2017. Privacy-Preserving Verifiable Set Operation in Big Data for Cloud-Assisted Mobile Crowdsourcing. IEEE Internet Things J. 4, 572–582. https://doi.org/10.1109/JIOT.2016.2585592

Zorbas, C., Eyles, H., Orellana, L., Peeters, A., Mhurchu, C.N., Riesenberg, D., Backholer, K., 2020. Do purchases of price promoted and generic branded foods and beverages vary according to food category and income level? Evidence from a consumer research panel. Appetite 144, 104481. https://doi.org/10.1016/j.appet.2019.104481

APPENDIX A: ETHICAL APPROVAL

Dear Emmanuel,

Research Ethics Application Approval: 1516/348 – *Differences in Perceived Information Sensitivity During Smartphones Use Among UK University Graduates".*

Your application to gain ethical approval for research degree activities has been considered and APPROVED by Prof Mark Lemon.

Please be aware that changes to the project plan or unforeseen circumstances may raise ethical issues. If this is the case it is the researcher's duty to repeat the ethics approval process.

Kind regards

Anne

Anne Smith

Research Coordinator

Research & Innovation Office (GH 4.64)

Faculty of Technology

DE MONTFORT UNIVERSITY

Gateway Building

The Gateway

Leicester LE1 9BH

UK

T: +44 (0)116 250 6519

E: amsmith@dmu.ac.uk

W: dmu.ac.uk

APPENDIX B: SAMPLE CONSENT FORM

Issue	**Respondent's initials**
I have read the information presented in the information letter about the study "Differences in Perceived Information Sensitivity During Smartphones Use Among UK University Graduates."	
I have had the opportunity to ask any questions related to this study, and received satisfactory answers to my questions, and any additional details I wanted.	
I am also aware that excerpts from the interview may be included in publications to come from this research. Quotations will be kept anonymous.	
I give permission for the interview to be recorded using audio recording equipment.	
I understand that relevant sections of the data collected during the study may be looked at by individuals from De Montfort University. I give permission for these individuals to have access to my responses	

With full knowledge of all foregoing, I agree to participate in this study.

I agree to being contacted again by the researchers if my responses give rise to interesting findings or cross references.

No ❑

Yes ❑

If yes, my preferred method of being contacted is:

Telephone: …….

Email: …….

Other: …….

Participant Name		Consent taken by	
Participant Signature		Signature	
Date		Date	

Appendix C: Westin's Original Interview Questions and the Analysis Guide

Westin's Original Questions

12 a. Consumers have lost all control over how personal information is collected and used by companies.

- Strongly Disagree
- Somewhat Disagree
- Somewhat Agree
- Strongly Agree

12 b. Most businesses handle the personal information they collect about consumers in a proper and confidential way.

- Strongly Disagree
- Somewhat Disagree
- Somewhat Agree
- Strongly Agree

12 c. Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.

- Strongly Disagree
- Somewhat Disagree
- Somewhat Agree
- Strongly Agree

Westin's Index Analysis Guide

Westin used the following definitions for classifying the public into three categories:

1. Privacy Fundamentalists are respondents who agreed (strongly or somewhat) with the first statement (12a) and disagreed (strongly or somewhat) with the second (12b) and third statements (12c – 3).

2. Privacy Unconcerned are those respondents who disagreed with the first statement (12a) and agreed with the second (12b) and third statements (12c).

3. All other respondents were categorised into Privacy Pragmatists.