



<http://researchcommons.waikato.ac.nz/>

Research Commons at the University of Waikato

Copyright Statement:

The digital copy of this thesis is protected by the Copyright Act 1994 (New Zealand).

The thesis may be consulted by you, provided you comply with the provisions of the Act and the following conditions of use:

- Any use you make of these documents or images must be for research or private study purposes only, and you may not make them available to any other person.
- Authors control the copyright of their thesis. You will recognise the author's right to be identified as the author of the thesis, and due acknowledgement will be made to the author where appropriate.
- You will obtain the author's permission before publishing any material from the thesis.

**Preteens' concepts and development of privacy,
and the relationship to decisions and actions
undertaken in online social environments
and with digital devices.**

A thesis

submitted in partial fulfillment
of the requirements for the degree

of

Master of Education

at

University of Waikato

by

ANGELA WEBSTER



THE UNIVERSITY OF
WAIKATO
Te Whare Wānanga o Waikato

2016

Abstract

A concern for privacy, the development of this, and how it becomes interpreted in offline and complex online environments has potential implications on young people's wellbeing and safety. Media often bring to attention more negative aspects of young people's privacy in relation to their online pursuits, which raises questions about perceived risks to one's privacy and actual risks encountered online and any subsequent implications. This study looks at preteens' broad concepts and development of privacy, and any relationship(s) these may have on their use of digital technologies and decisions and actions in online social contexts. A review of literature related to preteens' involvement in online social networks and issues of privacy presents a growing body of information, however, a scarcity of literature related to preteens' concern for privacy, and the development of privacy concern, suggests this study offers new insights in this particular area.

Students (N=60) aged between 11 and under 13 years from three provincial New Zealand schools participated in this qualitative study, and key data were gathered through a survey. Preteens indicated they valued privacy and specified its importance across dimensions of self. Furthermore, a desire for autonomy and control in managing aspects of privacy in their offline *and* online worlds was evident. However, concerns were raised regarding preteens' perceived capabilities and their actual competencies and knowledge of the technical, social, and ethical complexities presented online and in the use of devices. Also evident were inconsistencies in the types of support needed to care for the safety and wellbeing of young people. This suggests young people continue to need regular and robust support from agencies they themselves identified as important, and included caregivers, schools, and peers.

Opportunities to further develop caregivers' skills and knowledge is recommended, so they may better understand the crucial role they have in supporting the safety and wellbeing of their child in their exploration of complex digital environments. Their role is essential in positively contributing to the development of a concern for privacy. Recommendations are made, for schools, educators, and education policy makers in their role in this development. These include sustained teaching and learning opportunities across all learning levels in building related skills and competencies. Sourcing perspectives from preteens themselves as the experts of their ideas, experiences and knowledge, is integral to understanding how they navigate privacy issues when living lives both offline and online.

Key words: preteens, privacy, digital devices, online social networks

Acknowledgements

My interest in the complexities and challenges that arise and exist for different groups of people in relation to the evolving digital technologies used in schools and homes formed the motivation for this study. It is grounded in the belief that this area of interest matters, and that I may be able to contribute to this body of knowledge. I wish to acknowledge and thank those whose support and specific roles have been integral to this thesis.

To those students, teachers, parents, and schools who gave consent, time, classroom space, and effort to respond to the requests, forms, and the survey, I am most grateful. The students' enthusiasm was inspiring, and their comprehensive responses provided an abundance of data that has been invaluable.

Thank you to Garry Falloon, Associate Professor at the University of Waikato School of Education, for his professionalism and insight. His critique and support was thorough, tireless, and deeply appreciated. Thank you to Alistair Lamb, Waikato University librarian extraordinaire whose knowledge and patience was appreciated more than I could convey.

The financial support I received from the WMIER (Wilf Malcolm Institute of Educational Research) Masters Scholarship was integral to meeting needs incurred across the year, having stepped out of the classroom and any financial support to focus on this study fulltime. I was most grateful for this provision and the affirmation through the Scholarship, that this is an important area of research.

I wish to acknowledge my best friend and husband, whose shared belief in the purpose of this study, provided a much needed rudder at times when the 'waves loomed larger than than the boat'. I thank our two daughters for their encouragement and support, and who were instrumental in spring-boarding my interest in complexities arising for young people, technologies, and the online world. To my precious parents and dear friends who have offered unwavering encouragement and support, I express heartfelt gratitude.

Table of Contents

Abstract	i
Acknowledgements	ii
Table of Contents	iii
List of Figures	vi
List of Tables	vi
Chapter One: Introduction	1
1. Focus for the Research	1
2. Researcher Role	3
3. Significance of this Study	4
4. Structure of this Thesis.....	7
5. Summary	7
Chapter Two: Review of the Literature	8
1. What is Privacy?	8
1.2 Privacy and Preteens	12
2. Development of Privacy.....	13
2.1 Aspects of Privacy	15
2.2 Influences in Privacy Development	16
3. Complexities in Managing Privacy in Online Environments	18
3.1 Underage Users and Age Restrictions.....	18
3.2 Online ‘Playground’	19
3.3 Exposure to Online Content, Conduct, and Contact	20
3.4 Disclosure, Visibility and Online Audiences	21
3.5 Tools, Settings, and Challenges to Security and Privacy Online.....	23
4. Support in Complex Worlds.....	25
4.1 The Role of Caregivers	26
4.2 The Role of Schools	30
4.3 Other Organisations	32
4.4 The Agency of Young People	33
5. Summary	34
Chapter Three: The Research Design	36
1. The Research Questions	36
2. Theoretical Position	36
3. An Interpretive Paradigm	37
4. A Qualitative Approach	38
5. Research Methods and Instruments	39
5.1 Research Methods	39
6. Ethical Procedures.....	43
6.1 Access and Acceptance	43
6.2 Informed Consent, Assent and Confidentiality.....	44
6.3 Harm.....	45

7. Validity and Trustworthiness	46
7.1 Challenges to Validity and Trustworthiness	47
8. Data Coding and Content Analysis	48
9. Summary	52
Chapter Four: Findings	53
1. Demographic Information	53
2. Concepts, Examples, and Influences Related to Privacy	54
2.1 What is Privacy?	54
2.2 Importance of Privacy in Participants' Lives.....	57
2.3 Perceptions of Privacy Importance	60
2.4 Influences in Development of Privacy	62
3. Digital Devices, SNSs, and Caregiver Mediation/Oversight	66
3.1 Digital Devices	66
3.2 SNSs/Apps, Creation of Accounts, and Age Restrictions	67
3.3 Caregiver Mediation and/or Oversight.....	70
3.4 Mediation and/or Oversight Strategies Employed by Caregivers.....	72
4. Perceptions, Online Actions, and Influences	76
4.1 Actions Relating to P.I, Online Experiences, and Device(s)	77
4.2 Online Experiences	79
4.2.1 Concerns Encountered Online	82
4.2.2 Actions Undertaken in Response to Online Concern.....	84
5. Knowledge and Use of Online Tools and Settings, and Perceived Competencies	87
5.1 Online Tools and Settings	87
5.2 Status of Profiles and Awareness of 'Public'	89
5.3 Attitude and Capability in Using Specific Online Tools and Settings...	90
5.4 Perceptions of Capability in Management of Online Privacy.....	92
6. Summary	92
Chapter Five: Discussion	94
1. What is Privacy?	94
1.1 Importance of Privacy	96
2. Privacy Aspects Across the Personal, Social, and Physical Self	97
2.1 The Personal Dimension	97
2.2 Dimensions of Privacy: The Social Dimension	102
2.3 Dimensions of Privacy: The Physical Dimension.....	103
3. Development of Privacy Concepts.....	104
3.1 Influences in The Development of Participants' Privacy Concepts.....	105
4. Devices and Underage Involvement on SNSs/Apps	107
5. Caregiver Mediation and Oversight	110

6. Conduct, Contact, and Concerns Related to Devices and the Online Environment.....	112
6.1 Online Disclosure and Visibility of Personal Content.....	114
6.2 Online Conduct, Contact and Subsequent Concerns	116
7. Inter-relatedness Between Preteens' Private Offline Self, Preteens' Online Self, and Influencing Factors	119
8. Summary	121
Chapter Six: Conclusion, Implications and Recommendations	123
1. Summary of the Study.....	123
2. Implications for Caregivers, Educators, Organisations, and Young People	125
3. Limitations of the Study.....	128
4. Areas for Future Research.....	129
5. Conclusion.....	130
References	133
Appendices	146
Appendix A: Preteens and Privacy Survey	146
Appendix B: Mapping of Survey Questions	153
Appendix C: Survey Procedure Script	154
Appendix D: Study Overview and Introduction Note to Caregivers	155
Appendix E: Parental Information and Consent Form.....	156
Appendix F: Head of School and Supervising Teacher Information and Participation Consent Form	159

List of Figures

<i>Figure 1. A model indicating the shifting relationships between preteens' private-self, contexts, and influences, in the development of privacy concern.....</i>	120
---	-----

List of Tables

Table 1. <i>Summary Example of the Coding Process with Qualitative Data</i>	50
Table 2. <i>Demographic Data of Survey Participants</i>	54
Table 3. <i>Categorized Comments of Participants' Concepts of Privacy.....</i>	56
Table 4. <i>Qualitative Comments Categorized, of Privacy Importance in Participants' Lives</i>	59
Table 5. <i>Participants' Perceptions of Importance of Privacy</i>	61
Table 6. <i>Participants' Perceptions in Comparisons of Privacy Needs.....</i>	62
Table 7. <i>Perceived Influences on Development of Participants' Privacy Concepts and Behaviours.....</i>	64
Table 8. <i>Ownership and Type of Digital Device(s) Participants Use to Access the Internet</i>	67
Table 9. <i>Participants' Use of SNSs/Apps, and Comments Indicating Favourite SNSs/Apps</i>	68
Table 10. <i>Participants' Profile and/or Account Creation, and Awareness of Age Restrictions on Favourite SNSs/Apps.....</i>	70
Table 11. <i>Caregiver Access to Participants' Device(s), and SNS/App Accounts or Profiles</i>	71
Table 12. <i>Caregiver Access to SNS/App Accounts or Profiles Participants Use</i>	72
Table 13. <i>Participants' Qualitative Comments Categorized, of Caregiver Mediation and Oversight Relating to Participants' Use of Digital Device(s) and Online Activity.....</i>	74
Table 14. <i>Participants' Perceptions of Caregiver Awareness Regarding Their Online Activities</i>	76
Table 15. <i>Actions and Decisions Relating to Personal Information, Social Contexts Online, and Device(s).....</i>	79
Table 16. <i>Participants' Online Experiences, Degree of Concern, and Subsequent Action</i>	81

Table 17. <i>Participants' Qualitative Comments of Sources of Online Concerns, Categorized</i>	83
Table 18. <i>Participants' Qualitative Comments Categorized, Relating to Actions</i>	85
Table 19. <i>Participants' Use of Privacy and Security Tools on Device(s)</i>	88
Table 20. <i>Participants' Personal Information in Public Profiles on SNSs/Apps</i>	89
Table 21. <i>Participants' Knowledge and Use of Online Privacy and Security Tools</i>	91
Table 22. <i>Participants' Perceptions of Capability in Managing Their Online Privacy and Safety</i>	92

Chapter One: Introduction

This chapter outlines the focus for the research, the role of the researcher, and the significance of the study, how the study was structured, and concludes with a summary of the chapter.

1. Focus for the Research

This study is the outcome of a long-held interest in the complexities for young people, caregivers, and schools that have evolved through the introduction of mobile digital technologies paired with the seemingly high levels of autonomous access to these, and the challenges and opportunities many online environments present. While many younger people may appear to navigate the functions of digital devices and online environments confidently, this has not necessarily denoted competence and maturity in managing the social and technical complexities in these same environments (Livingstone, 2014; Yan, 2009). Such complexities have led to new laws within the New Zealand context with the introduction of The Harmful Digital Communications Act 2015, with the intent to provide a measure of protection and readdress for all citizens (Harmful Digital Communications Act, 2015). In addition, the eLearning Planning Framework is a Ministry of Education initiative designed to guide schools in their efforts to help develop media literacies, eLearning opportunities, and citizenship skills (Ministry of Education, 2010). However, this provides only a guideline or framework, and is not mandated across all schools and levels as curricula.

There is an increasing awareness of the need for young people to develop a range of skills, competencies, and ethical behaviours to support their online activities and connections with others. As an educator, I considered privacy aspects integral in some of these skills and behaviours. However, I sought to know what preteens thought about privacy, and how *they* believed these concepts and behaviours had developed, and what impact these had on their actions and decisions in online environments.

Therefore, the concept of privacy, what it is, how it is valued, and how it develops into behaviours in young people, is one of the key enquiries of this study. In addition, the study examines any relationships these concepts may have with how preteens engage with digital devices, and online social networks. It is concerned with connections and/or inconsistencies that may exist in preteens' understandings and concerns for privacy across offline *and* online contexts.

Seeking this understanding from young people themselves was a goal of the study, which involved sixty preteen students from three different schools (an equal number of boys and girls) all living in the same provincial city in New Zealand. The data and findings were sourced from a survey, and a qualitative approach to analysis was adopted. The key research questions were:

What were preteens' concepts of privacy and how might these have developed?

How do these concepts relate to their actions and decisions undertaken in online social environments and with digital devices?

Foci relating to the research questions were:

- 1.1 Exploring preteens' concepts of what privacy is;
- 1.2 Investigating how these concepts may have developed.
- 1.3 Determining what devices and online social networks are used;
- 1.4 Examining the role others have in supporting and influencing preteens in their use of devices and online social networks;
- 1.5 Exploring preteens' depth of knowledge and use of online settings and tools.
- 1.6 Exploring preteens' experiences of online challenges in which privacy can be difficult to maintain or navigate;
- 1.7 Inquire into the degree of confidence and competence preteens perceive they have in relation to managing privacy in online environments;

2. Researcher Role

This study is relevant to my role in the education sector. I have been in the education sector for much of my career, holding different roles and leadership positions, particularly in eLearning. As an early adopter of Internet-connected technologies and online sites in learning and teaching environments, and in my personal life, I used these for both social and educational purposes. Over time as these technologies evolved, I became aware that some students were engaging in concerning activities, for example - inappropriate disclosures on age restricted social networks, which were visible to the online public. There was an absence of information for users regarding online privacy, safety, and security in the very early days of social network sites such as MySpace, Bebo, and Facebook. With the introduction of mobile digital technologies and the growing prevalence and access to the Internet that young people were achieving, it appeared that some young people were spending time ‘unsupervised’ in these new digital environments. School communities I was associated with were struggling to keep up with ensuing challenges that were arising for their children. These included underage participation on social network sites used also by adults, a lack of knowledge or use of privacy settings, disclosure and the nature of content being uploaded, unwanted contact, online harassment, and challenges in competently handling potentially harmful online situations. A ‘divide’ was expressed by some caregivers who shared their anxiety and concern regarding their perceived lack of awareness and competency in using or having any knowledge of these technologies. This contrasted with the apparent confidence and scale in which their children could and were using these technologies.

Through forums and workshops, I voluntarily assisted schools and their specific communities with the goal to help equip staff, caregivers, and children to develop enterprising, resourceful, and resilient tools and strategies when online. This included exploring a variety of approaches in dealing with challenging situations online that required aspects of empathy, action, independence, negotiation, privacy, disclosure, awareness of laws, and personal integrity. My knowledge of social network sites and devices and the associated tools and settings was

relatively comprehensive, and I believed these to be complex and somewhat difficult for younger people to know and navigate, irrespective of their own values related to privacy. Furthermore, the notion of privacy and what it meant to young people were questions I sought answers to, as I perceived these to be core issues in some of the online challenges students were encountering. These were questions such as: What is privacy to young people? Did they attach value to it? Was there a relationship between their ideas about privacy, and their actions and activities online? If so, what were these? If there are incongruences, why might this be so?

This curiosity and concern led me to undertake postgraduate study, so that I might become better informed of others' theories, research, and outcomes. I believed deeper study could increase my knowledge and understandings, thus better equip me to support and encourage young people, caregivers and schools in their responsibilities and endeavors in this particular area. This desire provided the impetus for me to undertake this research study.

The next section discusses the significance of this study.

3. Significance of this Study

By undertaking this study, I sought a more detailed understanding of what privacy was to preteens (those aged between 11 and 13 years), if it was valued, and how these concepts may have developed. In addition, I sought to understand the nature of any relationship between their activities and experiences using digital devices and engaging in online social networks, and their concepts of privacy. I posited that if we knew more about what privacy was to younger people, and how they may have developed these concepts, this knowledge might be important in tailoring discussions, learning opportunities, resources, and curriculum relating to the management of privacy across offline and online contexts. Furthermore, those who have responsibilities in educating, and shaping young lives may potentially benefit from the information outcomes of the study.

This study notes that there is limited research and literature that has described or explained how privacy is perceived by preteens, and in particular, seeking this understanding from the perceptions of young people themselves. Literature that has been published has largely overlooked the agency of children's voices (Shmuell & Blecher-Prigat, 2011; West, Lewis, & Currie, 2009). Conversely, there is a growing source of literature related to young people's *online* privacy behaviours (Madden, Cortesi, Gasser, Lenhart, & Duggan, 2012; Youn, 2009). The gap that exists in literature and research relating to children and preteens' privacy perspectives and their development of a concern for privacy, points towards this study as providing new considerations and opportunities in understanding young people's views and knowledge of privacy.

Privacy is complex and difficult to define, however there appears to be some consensus that privacy has *types* and *functions*, and is a socially negotiated activity influenced by cultural factors (Altman, 1977; Inness, 1992; Kemp & Moore, 2007; Schoeman, 2008). It is also an integral aspect of self identity, and woven into aspects of the cognitive, social, emotional, spiritual, physical and moral development of self (Harter, 2012; Moshman, 2011; Smetana, 2010). As many younger people's lives are now lived both offline and online, complexities imposed by the Internet and online social networks pose new challenges to their privacy as they move seamlessly between these contexts. This suggests that new understandings of more contemporary views of privacy are required. Negotiating new privacy concepts and behaviours in response to the challenges and competing elements that online environments present today are essential (Kemp & Moore, 2007; Solove, 2002). This is particularly pertinent in this digital environment in which participants and other young people appear to have a ubiquitous mobile connection to online global audiences (Lenhart, 2015; Livingstone, 2015).

Media and other literature may at times summon public panic in relation to potential risks encountered online, however recent literature is challenging the assumptions that online risks equates to harm, and opposes over-reactions that lean towards a risk-adverse society (Finkelhor, 2014; Livingstone & Smith, 2014).

An important aspect in the development of healthy, resilient, confident young people is their ability to negotiate risks and explore opportunities in the online environment as well as offline, and risk-adverse environments limit the development of necessary skills (Livingstone & Smith, 2014).

Literature supports the need for developing specific and general skills and characteristics that may enable younger people to make considered choices and take evaluated risks both offline and online. This is particularly so if they are to develop a ‘concern’ for privacy, which is a key determinant in the degree of online disclosure (Liu, Ang, & Lwin, 2013). This task falls primarily on caregivers, schools, and organisations, as stakeholders in the welfare of young people. Caregivers are parenting in challenging and exciting times, however the consequences of the often ubiquitous access many younger children have to digital devices and the Internet is unknown at this point in time (EU Kids Online, 2014). Challenges experienced by some caregivers include a lack of technical knowledge, limited understanding of the new forms of socialisation online for young people, or recognising that participation online is “an extension of their offline lives” (O’Keeffe & Clarke-Pearson, 2011, p. 801).

The complexities involved in parenting, teaching, and governing in a technology rich society means collaborative solutions and integrated approaches are necessary if younger people are to acquire the skills and develop attitudes essential to becoming confident, autonomous, and contributing adults. By examining preteens’ privacy concepts, and in addition, their activities and experiences in their use of digital devices and online social network sites, it is hoped that a clearer understanding of their perspectives, capabilities, and challenges may evolve, and in turn, inform those who are tasked with the care and protection of young people.

The next section explains the structure of this thesis.

4. Structure of this Thesis

This thesis is organised into six chapters. The first chapter provides an overview of the study and shares the motivation of the researcher for sharing this work. The second chapter reviews the literature, and examines other theories, research, and outcomes in relation to the findings in this study. The design of the research and data-gathering tools that were chosen, the make-up of participants, the ethical considerations, and aspects of validity and trustworthiness, are detailed in the third chapter. The findings and the data from the survey are outlined in the fourth chapter, and key issues and the nature of relationships within the data are discussed in the fifth chapter. In closing, the sixth chapter notes the conclusions that are drawn and makes recommendations, while also acknowledging the limitations of the study. Further research within this particular focus is also discussed in this last chapter.

The next section summarises this chapter.

5. Summary

This chapter provided an overview of the study, and described the motivations for this research, the context, and the structure of the study. The need for a more salient understanding of the complexities involved for younger people in navigating complex online environments in relation to their privacy and safety, and the need to support young people in developing a ‘concern for privacy’, were outlined. In addition, the responsibility tasked to caregivers and schools in this development was noted. The premise is that these groups may in turn be better informed of their particular role in this shared responsibility.

The next chapter provides an overview of the literature in the field relating to key enquiries within this study.

Chapter Two: Review of the Literature

Introduction

The advent of Internet-connected technologies in conjunction with the mobility of devices has ushered in new and evolving challenges related to privacy, and the management of this in offline and complex online environments, particularly for younger people. Privacy and how it is conceived, valued, and developed by preteens, are key focuses in this study, and in addition, the relationship(s) between preteens' privacy concepts and their interactions with digital devices, and online social environments.

This chapter examines literature and research related to privacy, the development of privacy concepts, influences, and management of privacy online. The first section examines theories of what privacy is, particularly to younger people. The second section describes theories relating to the development of privacy concepts, aspects of privacy, and influences in privacy development. The third section examines underage use of online social networks, and complexities involved for young people in navigating and managing their privacy and security online. The fourth section looks at literature related to crucial influences and support for young people in understanding online complexities.

1. What is Privacy?

Discourse related to privacy can be found in literature relating to philosophy, law, psychology, education, politics, history, science, anthropology, religion, medicine, sport, technology, and more. One's right to privacy was seen in the writing of Brandeis and Warren in 1890, who in response to the prying of journalists and photojournalists looking for tawdry 'news', created a 28 page outline of the need for law to be established to protect one's right to privacy, and thus the concept of intrusion of privacy was borne (Bratman, 2002). Privacy, with roots in ancient civilizations and animal kingdoms, was theorised as an imperative and right of individuals and has a history of being both valued and contested (Westin, 1967).

Privacy was described as having types and functions serving purposes needed by individuals and groups, through to organisations and governments (Westin, 1967). The emergence of modern industrial societies created new opportunities for physical and psychological opportunities for privacy to develop, and was seen as being shaped by cultures and sub-cultures as well as individual needs. Too much privacy could be alienating, while too little might create a sense of invasion of oneself, confirming Westin's (1967) theory of the shifting distances seen in states of solitude, intimacy, anonymity and reserve. The concept of one's right to privacy was seen historically in western societies, whereby the origins of privacy relating to one's body was linked with one's right of protection over their body, and laws were established to support this. Overtime this evolved to include the right to make decisions about one's body across a raft of issues in which concealment or regulation of disclosure was desired (Kasper, 2005). Laws were scripted and have been upheld in many countries around the world, providing measures of protection of 'privacy', as defined by the particular contexts and laws of that nation and in some instances, the rights of the state that preside over personal privacy rights.

The influence of culture on privacy concepts and behaviours was theorised by Altman (1977) as being much more than one's own culture, and included the notion of a much larger "holistic culture" (p. 70) shaping the processes involved in achieving privacy through regulating social interactions with others. Altman (1977) believed that greater influences steer desired or appropriate levels of openness and closure of privacy boundaries, and are shaped by the cultures one is affiliated with. This includes where one lives in the world, the organisations and groups one belongs to, and the closest of cultures, that of family and peer groups. Altman's (1977) theory purported that people need social exchanges that in turn, require control over boundaries and access of others, while also providing opportunities for disclosure. Therefore, privacy could be described as the controlling of access of others through boundaries surrounding one's personal realm. Similarly, disclosure is also controlled through such boundaries, although external parameters granted to an individual, group or nation may influence these processes.

The functions of privacy need to be understood, however content of privacy is also important, as functions of privacy such as separation and control are very different concepts and draw on moral tenants, according to Inness (1992). This is seen in case law which adopts the perspective that value of privacy stems from creating environments in which happiness can be pursued, and includes health and safety in the home (Inness, 1992). It is the ‘parameters’ of privacy that enable secret or intimate facts about one-self to be kept from the prying eyes or ears of others, and in turn, personal relationships can be fostered. Law also acknowledges that value for privacy originates from respect for the spiritual nature of humankind, and “individual dignity” (Inness, 1992, p. 18). However, privacy is not necessarily a stable concept, and is susceptible to change through internal and external conditions relating to intimate information, access, and decisions (Inness, 1992). This aligns in part with Altman’s (1977) theory that dynamic boundary controls are regulated by the holistic cultural influences in our lives and environments that we inhabit. This is particularly germane in the dual realities lived in an online and offline world today.

Privacy is a complex, imprecise, and difficult notion to define, and difficulties have existed in defining privacy for over a century (Kemp & Moore, 2007). This is primarily due to complex and multi-dimensional aspects extending across physical, informational, and decisional privacy known also as individual autonomy, and the intricacies involved in conceptualizing, describing and managing these (Shmuell & Blecher-Prigat, 2011). The pursuit of defining privacy has often been critiqued. Reasons include being specified too narrowly or broadly, or examined through a cultural or historical lens which may result in inapplicability, or driven by a values focus which may produce outcomes reflecting researchers’ own biases or predetermined goals (Kasper, 2005).

Despite difficulties and constraints in defining privacy, others have sought to conceptualise what privacy is. Parker (1974) viewed privacy as extensive and particularised, and described it as the activity of controlling access others may have to aspects of self that can be elicited via one’s senses. The ability to listen in, survey, record, pry, and elicit information about others, involves one’s senses.

However, Parker's assessment can be challenged, as aspects of one's self are exposed to others' senses on a daily basis, simply because we see others, hear others, and view others' affairs, and many of these contexts do not imply privacy invasion. Schoeman (2008) outlined privacy as having two types, distinguishing between privacy 'for' someone or something, which enables one to develop themselves as well as their relationships, and privacy 'from', which involves the restriction of access by others. Parker's (1974) proposal of privacy, as something governed and moderated by one's senses, can be debated when drawing on the example of someone sitting on a bus who observes and listens to a conversation between those seated closely by. This does not infer a breach of privacy has occurred, rather, it cements the theory that privacy boundaries are firmly related to the nature of relationships (Altman, 1977; Schoeman, 2008).

In defining privacy, no definitive parameters have been described and it continues to be regarded as a complex concept, serving many different purposes and needs (Inness, 1992). The value and protection of privacy has seen nations, groups and individuals employ diverse means and strategies to maintain, or at times invade others' boundaries. History shares that at times, these strategies have resulted in the disclosure of highly sensitive content, initiating complex court cases or conflict on battlefields. An example can be seen in 'whistle blower' Julian Assange who continues to reside in the Ecuadorian embassy in London. Assange sought protection due to criminal charges held against him that he purports were generated as a result of his disclosure of highly classified material through WikiLeaks, the site known for publishing highly sensitive information to the public domain (Pilger, 2013). The literature suggests privacy is a right of the individual, a necessity for relationships to flourish and individuals to maintain wellbeing. However, it is only preserved and sustained in relation to the cultural, political, environmental, and personal contexts of one's life at any given time.

1.2 Privacy and Preteens

Preteen, is defined as those aged around 11 and 12 years of age (preteen, 2015). The research in this study was two-fold, with the first section investigating participants' broad concepts and perceptions of privacy, how these may have developed and whether privacy was valued, and if so, to what degree. In researching other studies and literature in relation to young peoples' privacy perceptions and concepts, it became apparent that a scarcity of research and literature existed in this domain, and was an unexpected finding. Furthermore, *any* data elicited of younger people's privacy concepts and perceptions in the context of life offline was limited. This aligns with other studies that purport research on children's privacy is limited, and has been based on the perspectives and perceptions of adults, subsequently overlooking the agency of children themselves (Shmuell & Blecher-Prigat, 2011; West et al., 2009). However, a growing source of literature and research into young people's *online* privacy behaviours is accessible, and provides valuable data and recommendations for stakeholders involved in young people's wellbeing and development. The gap that exists in literature and research relating to children and preteen privacy perspectives in *offline* contexts, points towards this study as providing new considerations and opportunities to understand privacy of young people across all contexts of their lives.

This raises the issue that children and adolescents' concepts of privacy have largely been founded on the assumptions of adults, which in turn has formed the basis of research and literature to date. This is supported by Shmuell and Blecher-Prigat (2011) who state that "there is widespread consensus that children show less concern than adults about privacy...however very few empirical studies have demonstrated this" (p. 761). This consensus and lack of supporting data is problematic, and contrasts with the findings in this study, which showed most participants held high regard for privacy and had mature concepts of what privacy is. In researching children's perspectives, behaviours, and perceptions, the use of participatory methods draws on the tenet that it is the children themselves who are

most expertly situated to provide insights into their world (Burke, 2005; Clark & Moss, 2011). That there is an absence of participatory methods in prior research in ascertaining what young people perceive privacy to be, the degree to which it is valued, and how concepts may have evolved, indicates there is a void of data elicited from those most closely connected with their own notions and perceptions. To develop a deeper understanding of privacy issues, children and young people need to be the source and subject of the research where possible, without the intermediary of parents, teachers, and others.

In contrast, research relating to children, teens, and privacy in online environments and contexts is abundant, with different research methods being employed, including the agency of young people's voices (Livingstone, Kirwil, Ponte, & Staksrud, 2014). The findings of this study signify there is a basis for considering new approaches in discussing privacy issues across *offline* and *online* contexts with stakeholders, and in particular, young people. These are further discussed in the Conclusion and Recommendations chapter of this study.

2. Development of Privacy

Different factors are involved in the development of privacy concepts and how these translate into behaviours that are exhibited across various contexts. Privacy is considered to be a facet of identity development comprising cognitive, moral, social, and emotional developments, according to theories posited by childhood, cognitive, and morality development theorists, Jean Piaget, and Erik Erikson (Gibbs, 2013; McLeod, 2013; Meadows, 1986). Kohlberg, also a developmental theorist, saw privacy as an aspect of moral reasoning, which he described as a series of six stages and three levels from the earliest stages of childhood and into adulthood, although not necessarily a sequential development across a lifespan (Cherry, 2015a; Gibbs, 2013). Individualism and Exchange, the stage of making moral decisions based on one's own interests may see privacy concepts and ensuing behaviours as shaped by perceived benefits to the individual. Similarly, the stage of Interpersonal Relationships in which decisions are made based on others' impressions of one-self, may provide a basis in which privacy perceptions

and behaviours are shaped by efforts to manage impressions of self to others. These stages provide an interesting theory, particularly in relation to the actions of some participants in this study who indicated they were very concerned about an online encounter or occurrence, but chose to do nothing in response to this concern. Other studies also align with this absence of action or response (Cox Communications, 2014; Lenhart et al., 2011a).

Psychologist Jean Piaget, known for cognitive development theories, believed a relationship between privacy and moral reasoning existed and noted that aspects of autonomy appeared to be derived from a moral basis, which in turn motivated adolescents to act on their perceived need of privacy (Reed, Turiel, & Brown, 2013). Piaget outlined the theory of cognitive schemas as a way of understanding how individuals develop their own knowledge and understanding across spheres of the emotional, spiritual, cognitive and physical realms (Cherry, 2015b). Privacy schemas are constructed over time from experiences, observations, and influences, and can be modified or altered through the introduction of new information or experiences, thus building a 'reference' or schema of privacy meaning and autonomous privacy behaviours. It is important if this theory has rigor, to consider that privacy schema may be founded on positive and/or negative input that may potentially create vulnerabilities or predispositions in the privacy behaviours of young people in offline and/or online contexts. For example, negative experiences encountered online have influenced some young people's perspectives and practices, and as a result, causing them to trust less and manage privacy controls more deliberately (Christofides, Muise, & Desmarais, 2012).

Autonomy and control are key factors in Erikson's theory of psychosocial stages, purporting that children grow through various challenges encountered at different stages, and if these challenges are successfully met, independence and self-efficacy strengthens (McLeod, 2013). Preteens experience a range of challenges across the personal, social, and physical dimensions as their bodies are in states of change, social connections are becoming central, and many other demands such as schooling, home, and 'online' life, are encountered. If, as Erikson claims, earlier childhood experiences related to development of

self-identity have been relatively successful, a sense of autonomy and control are more likely to be achieved (McLeod, 2013). Literature and research clearly indicate that privacy concepts and behaviours develop over time, throughout childhood, adolescence, and into adulthood in response to internal and external determinants. The evolution of privacy concepts happens in conjunction with developments of self and identity, and includes aspects relating to the physical, cultural, emotional, moral, social, cognitive and environmental characteristics (Harter, 2012; Moshman, 2011; Parke & Sawin, 1979; Smetana, 2010).

2.1 Aspects of Privacy

Key aspects of privacy have been discussed in literature and many of these were identified in the findings of this study. Personal factors that are managed through autonomy and control, such as one's thoughts, one's property, one's personal information, one's relationships with others, one's body, and one's safety are all aspects of privacy, and often incorporate boundaries established to maintain and protect these factors (Kasper, 2005; Magi, 2011; Smetana, 2010; Solove, 2002). In addition, others' responses towards one's privacy boundaries can lead to a sense of invasion and loss of control (Hawk, Keijsers, Hale 111, & Meeus, 2009; Parke & Sawin, 1979; Smetana, 2010).

Solitude and space have been noted as important aspects of privacy, and provide the space for retreating from others' access and interference, which in turn aid a sense of well-being (Hodkinson & Lincoln, 2008; Livingstone, 2002; Margulis, 2003). Solitude seeks separateness in a time and place where one can decompress, be alone, and contemplate the interactions encountered through social contexts, experiences, and new information (Blatterer, Johnson, & Markus, 2010). However, juxtaposition exists between taking time and space to decompress and disconnect from others, and the tendency towards ubiquitous connectivity in today's Internet-connected mobile and digital landscape (Belsky, 2010; Turkle, 2011). Through the access many young people have to mobile

digital technologies and the Internet, studies suggest that teens are gravitating to fill these gaps with online activity, and engagement with online sites is “at times motivated by boredom” (Awan & Gauntlett, 2013, p. 120).

Personal information exchanged between individuals or groups is an aspect of privacy related to self-disclosure, and is socially negotiated and reliant on measures of trust. Secrecy and disclosure are dependent on motivations in which sharing is seen as desirable or beneficial, and can extend to large groups of people who are privy to sensitive information about something or someone. Altman’s (1977) theory, that privacy is a socially negotiated activity, is evident in relationships between people as they mediate aspects of concealment and self-disclosure, both being necessary in order for close bonds to be forged, and is a “ubiquitous and trans-cultural phenomenon” (Trepte & Reinecke, 2011, p. v). However, one’s right to privacy is at times forfeited through indiscretion or intended disclosure, and may create great conflict and distress. In the online environment, some employ anonymity or mask information through the mechanisms available within these sites, however anonymity or masking does not provide the means of maintaining or deepening relationships, which is a desirable aspect and key benefit of social network sites (SNSs) and applications (Apps) according to teens (Awan & Gauntlett, 2013).

2.2 Influences in Privacy Development

Wide-ranging influences attribute to the development of privacy, and include where one lives in the world, the political systems of the country one identifies with, ethnic and cultural parameters, one’s gender, age, and status (Kemp & Moore, 2007). Furthermore, Smetana (2010) explains that individualistic cultures which “include New Zealand...” (p. 97), promote independence, personal autonomy, personal goals, and self-reliance throughout its legal, educational, and political sectors, therefore appropriating privacy as a right (Margulis, 2003; Smetana, 2010). Children’s privacy in some countries is regulated and protected in measure across offline and online contexts through presiding laws and policies. Children living in countries belonging to the United Nations are protected by

UNCROC (The United Nations Convention for the Rights of the Child), which states they have the “right to legal protection from unlawful or unreasonable interference with your privacy (including personal information held about you), your family and your communications” as stated in Article 16 of the Children’s Commissioner (2003). This applies to children in New Zealand, who are given legal protection from any interference and harm from others regarding their individual privacy and personal information (Children’s Commissioner Act, 2003). Furthermore, the Harmful Digital Communications Act 2015 gives rights and protections to any victims of cyber-bullying who incur serious emotional harm as a result, and may potentially impact on people’s privacy, identity, and well-being (Harmful Digital Communications Act, 2015). Children in New Zealand may encounter harm or interference, and incidences ranging from most serious such as suicide, to more minor, have been reported (Green, Harcourt, Mattioni, & Prior, 2013; Ihaka, 2008).

Personal influences integral in the process of privacy development are highlighted in literature, and indicate the critical impact that family, friends, and other organisations have in shaping younger people’s notions and perceptions (Livingstone, 2015; Livingstone, Ólafsson, & Staksrud, 2013). However, as preteens move into early adolescence, personal issues become central and are negotiated more aggressively, as aspects of one’s private self are seen as “lying beyond the realm of legitimate societal regulation and moral concern” (Smetana, 2010, p. 70). Therefore, while a transition between caregiver oversight and mediation and adolescents’ expanding control over their preferences, choices, body, and self-expression is taking place, tensions and conflict are common. In families where there is regard for one’s boundaries over their personal domain, relationships are more likely to have cohesion and respect (Smetana, 2010). Conversely, where there are poor or harmful influences, some young people are vulnerable to developing skewed and potentially destructive concepts and behaviours across aspects of self and one’s personal domain. Caregivers, peers, schools and communities continue to play a crucial role in the development of

many aspects of self that are in flux during the early, mid and late adolescent stages, and not all influences are necessarily positive in the lives of young people (Spielhagen & Schwartz, 2013).

3. Complexities in Managing Privacy in Online Environments

Privacy on SNSs and online environments is often difficult to navigate and negotiate, and many competing factors provide challenges, particularly for ‘underage’ users. Issues younger SNS users face include complexities in understanding the social nuances of SNSs, technical intricacies, impression management, visibility of self to different audiences online, disclosure of personal information, negative encounters, and trust of others online. This section reviews these challenges and examines literature and research relating to these issues.

3.1 Underage Users and Age Restrictions

The prevalence of access that many teens and younger people have to Internet-connected mobile devices has been identified in studies; furthermore, young people spend a significant amount of time engaging with online sites, often without any supervision (Crothers, Gibson, Smith, Bell, & Miller, 2013; McGlynn, 2010). In addition, there is a prevalence of underage users on SNSs and Apps that require users to be over the age of 13 years, or older on some sites (Livingstone et al., 2013; Strom & Strom, 2012). Other studies demonstrate that usage of SNSs by teens and younger children is increasing overtime (EU Kids Online, 2014; Rideout, Foehr, & Roberts, 2010). The restriction of access to those under 13 years without written approval from legal guardians applies to all websites created and operating within the United States of America (U.S.A), and are the requirements of COPPA, the Children’s Online Privacy Protection Act (Children’s Online Privacy Protection Act, 1998). This requirement was in response to concerns arising from online marketing and organisations that sought to advertise and solicit to minors. Many U.S.A content providers now invoke an age restriction of 13 years and over, as it is untenable to verify permissions.

While U.S.A law may not apply to underage users outside of America, caregivers are encouraged to adopt these age restrictions, using them as guidelines for younger children (Vodafone New Zealand, 2016). In some countries the number of underage users of SNSs and Apps is linked with the prevalence of teenage SNS use (Livingstone et al., 2013).

In addition, underage users of SNSs have fabricated information in order to create an account or profile, or enlisted someone to do so on their behalf (Brown, 2011). Issues arise in relation to this and include ethical considerations involved in fabricating truth, exposure to content on sites which adults co-use, advertising directed at adult audiences, and the potential for unwanted contact by unknown and older users (Livingstone et al., 2013; Skinner, 2010). Preteens are described as an “emerging sophisticated online group” (Yan, 2005, p. 394). However, cognitive and social development associated with age groups, are dominant factors in the understandings of the Internet, degrees of technical competencies, and social awareness (Yan, 2005, 2006, 2009).

3.2 Online ‘Playground’

The most prevalent activities young people partake in online in order of popularity are visiting SNSs, watching video clips, using the Internet for school related purposes, and playing games online, according to one particular study involving a large number of 11-16 year old participants across multiple European Union (E.U.) countries (EU Kids Online, 2014). While devices may be used for learning purposes, entertainment and socializing are still the two most important motivations for youth and younger Internet users (Crothers et al., 2013). Many SNSs and Apps provide a playground and meet-up space that is accessible anywhere, anytime, and appeal to teens as well as younger children. Livingstone (2008) states, “It seems for many, creating content and networking online is becoming an integral means of managing one’s identity, lifestyle, and social relations” (p. 394). While mainstream media often report more negative and riskier aspects of privacy management on SNSs and the risky online pursuits of some young people, research has highlighted some of the positive aspects of

socializing and sharing online. In this stage of development where self-identity and negotiation of peer relationships is both important, and at times fraught with challenges, SNSs can provide “a medium through which they could express themselves openly without having to face negative repercussions, such as, embarrassment or humiliation” (Awan & Gauntlett, 2013, p. 122). This is particularly so for those who find face-to-face social interactions more intimidating and stressful, as SNSs/Apps provide a means of mediated connection where confidence for self-disclosure can grow and trust can evolve (Erdur-Baker, 2010; Kafai, Fields, & Ito, 2013).

3.3 Exposure to Online Content, Conduct, and Contact

Percentages of young people is increasing in relation to those who have been exposed to, or sought online content that may have disturbed and/or caused concern. Through causes such as a lack of filtering, customizing of settings, inadvertent browsing, intentional searching, observing others’ online activity, some young people have been exposed to distressing material online. This includes exposure to content known as User Generated Content (UGC), for example hate messages, pornography, self-harm sites, pro-anorexia sites, and opportunities in which cyber-bullies have struck within SNSs, blogs, games and other social sites (EU Kids Online, 2014). Content poses the greatest concern to those aged between 9-12 years of age, while contact and conduct is of greater concern to teens (EU Kids Online, 2014). The most concerning content for young people is that which exposes them to ‘real’ people, scenarios, and situations whereby someone or something is being tormented, bullied, humiliated, or harmed (or self-harmed). However, some who were exposed to fictional ‘horror’ images or video clips report concern (EU Kids Online, 2014). The ease with which younger people can ‘stumble’ upon disturbing content is considerable (Livingstone, 2015). Furthermore, negative experiences encountered online by younger people may have a more adverse impact compared to adults, as researchers conclude that young people are more vulnerable (Livingstone, 2014; Rainie, Lenhart, & Smith, 2012).

The greatest public concern is the potential for online contact that leads to bullying, and face-to-face meeting with someone previously unknown to a young person (boyd, 2014; Livingstone, 2013; Livingstone & Smith, 2014). While this is often sensationalised in media, it is a serious issue and studies report there are a number of young people who consider meeting up with someone they've only met online, and a smaller number who actually do (Cox Communications, 2014). Also, older youth are more likely to engage in contact with unknown others (Lenhart, Madden, Cortesi, Gasser, & Smith, 2013a). However, not all exposure to risk results in harm, and many factors interlink as to the nature of the risk, potential or incurred harm, and alarmist reporting can skew public perceptions (Finkelhor, 2014; Livingstone, 2014; Livingstone & Smith, 2014).

3.4 Disclosure, Visibility and Online Audiences

Substantial personal information is shared by teens on online SNSs such as their real name, interests, school, town or city, cell phone number, email address, birthdate, relationship status, or photos/videos of themselves (Lenhart et al., 2013a). While fewer teens indicate concern over third party access to their information, many report they actively manage their content on SNSs to reflect impressions of self they desire to promote to their audiences, while deleting less popular content depending on the number of 'likes', or negative comments (Lenhart et al., 2013a). Some youth with more narcissistic personality traits seek opportunities to 'stand out' and receive the desired attention, thus disclosing personal information more regularly and perpetuating a cycle of disclosure and attention (Liu et al., 2013). Participants in this study shared pertinent personal information on their SNSs, and while numbers were few, there is cause to consider the willingness or naivety in disclosing such information.

Issues of privacy arise in relation to what content and personal information is visible online, and to whom. Users do not necessarily know that many SNSs employ a range of default privacy settings that enable the 'public' to view content. Understanding the tools to customise these settings require a level of technical knowledge (Yan, 2005). Any understandings one may have of the social nuances

and challenges in online environments, does not appear to increase one's technical competencies to manage complexities of the Internet and online tools, and the younger the user, the less technically competent they are likely to be (Yan, 2006, 2009). Three significant variables emerged in one study that explored the degree of online disclosure and privacy made by younger SNSs users (De Souza & Dick, 2009). The first variable was peer pressure, and proved to be a persuasive influence on the degree of sharing online. Secondly, the design of the SNS itself, which encourages users to fill out 'required' fields and sections with key personal information. Thirdly, signaling, which is the motivation of a user to portray themselves in a certain way for an effect and therefore information disclosed is carefully managed and deliberate (De Souza & Dick, 2009). Both social understanding and technical competency is required to mitigate risks associated with one's privacy, safety, and security with often vast and unknown audiences (Yan, 2006, 2009). Reading and interpreting the Terms of Service on SNSs in order to understand how one's content may be used, shared, or deleted is essential but rarely undertaken (Peterson, 2015), and are not written for younger or struggling readers, nor 'underage' SNS users.

The visibility of personal content in the online public domain, as well as the large audiences many teens keep through adding 'friends' in SNSs are issues, and potentially make any disclosures online a very public affair. Livingstone (2008) presents an interesting perspective, stating that issues related to 'public' are for youth, "not so much a concern, notwithstanding media panics about 'stranger danger', as that of being visible to known but inappropriate others- especially parents" (p. 405). In contrast, one study indicates that almost three-quarters of participants were 'friends' with caregivers on a SNS, and where there was provision to customise what groups could view, most teens did not utilize this setting to differentiate content between caregivers and peers (Lenhart et al., 2013a). Furthermore, a relationship is indicated between the number of 'friends' one has on a SNS, and management of one's profile and reputation management according to the study, and findings suggest those with larger online audiences spend more time masking information and fashioning profiles and content (Lenhart et al., 2013a).

The effect of sharing widely online by millions of SNS users, may suggest the collective act of disclosure practices adopted by so many could change the “normative understanding of privacy from the ground up” (Blatterer et al., 2010, p. 92). The influence of norms is also suggest by Livingstone and Smith (2014), who propose that future research and practitioners look at “how a complex interplay among social norms and technological affordances shapes any particular communicative context” (p. 647).

Of particular concern is the tendency for younger users of SNSs to disclose more critical personal information (De Souza & Dick, 2009), and coupled with the issues relating to fabrication of age, this is potentially problematic. The motivation by younger users to socialise online, and the degree to which this is achieved positively, relate to a willingness to disclose personal information and in turn, privacy concerns are also lowered (Lwin, Miyazaki, Stanaland, & Lee, 2012). While the opportunity to explore, experiment, and self-disclose are motivating factors for youth and younger children to pursue an online presence, management of both risks and opportunities afforded through the technological mechanisms are required (boyd, 2014; Livingstone, 2008; Livingstone & Smith, 2014).

3.5 Tools, Settings, and Challenges to Security and Privacy Online

Issues can arise from naïve or relaxed attitudes towards privacy, safety, and online security by adults, teens, and younger children in relation to their devices, passwords, and personal disclosure online. In this study, a large number of participants indicated they had shared passwords and/or devices at times, and some indicated they didn't know how to adjust privacy settings, or didn't choose to. Literature suggests passwords are commonly shared with others, and can be seen as an extension of trust or intimacy (Lenhart et al., 2011b), however, in some cases passwords are also shared with unknown but ‘trusted’ others. This was evident in one study that showed that almost all of the adult participants at a particular workplace willingly gave their username to a ‘researcher’, and over half shared their password with this actor (Novakovic, McGill, & Dixon, 2009). Many

youth commonly share their passwords with others and coupled with the use of multiple SNSs, these factors potentially increases the risk of involvement in cyber-bullying (Meter & Bauman, 2015). However, as youth gain more experience they are less inclined to share passwords (Meter & Bauman, 2015). Age is a critical factor in the degree of competency and knowledge of technical tools and settings and use of these online, and is determined largely by the developmental stage of the user, with younger users demonstrating less capability than their older counterparts (Yan, 2006, 2009). Furthermore, when knowledge of privacy tools and settings is sought by young users, it has been primarily sourced from peers, or self-learned, although some seek advice from family members according to Lenhart, et al. (2011a).

However, while many young people may desire to customise their privacy settings, the design interface and technical affordances on online sites do not necessarily provide easy navigation, nor “subtle control over who has access to what information” (Christofides, Muise, & Desmarais, 2012, p. 716). In one study, teens aged between 12 -17 years indicated they cared about privacy online and believed they were highly capable in managing privacy concerns, while many used settings to ensure their SNS content was visible to their ‘friends only’, or ‘friends of friends’ (Lenhart, Madden, Cortesi, Gasser, & Smith, 2013b). Young people’s perceptions of the capabilities to manage technical and social complexities online may or may not be accurate, and in this study competency was reported as high, while inconsistencies were also evident in the findings in relation to safe and private online practices for some participants.

Strategies that can be undertaken online to secure one’s content and provide layers of privacy and safety, include the clearing of search History and Cookies, blocking unwanted contact, reporting behaviour to site administration, deleting ‘friends’ or content, deleting online accounts, and installation of monitoring or security software. However, some of these strategies such as clearing History or Cookies have also been used by some teens to prevent caregiver awareness of activities and encounters, and a small number have deactivated or deleted monitoring software from their device (Cox Communications, 2014).

The tensions and complexities at play in managing one's privacy, safety, and security online are evident, and are complicated by the desire for privacy by young users, from 'select' others who are required to ensure the safety and wellbeing of their children. As different studies yield some variances and alignments in findings, this suggests the cultural, geographical, political, technological, and social contexts in which young people operate within, influence privacy concepts and behaviours in online environments. Experiences shape behaviours, and young people are more likely to seek and implement privacy information and strategies online after encountering negative experiences, and a review of trust of others may also occur as a result (Christofides et al., 2012).

4. Support in Complex Worlds

An important aspect in the development of healthy, resilient, confident young people is their ability to negotiate risks and explore opportunities in the online environment, as well as offline. Mistakes are made in both contexts, however media and other stakeholders often perpetuate an assumption that online risks and negative encounters equate to harm. While there are accounts of actual harm occurring, the degree and frequency to which this occurs and the methods and measures used are not reliable enough to substantiate some of the claims (Finkelhor, 2014; Livingstone & Smith, 2014).

Risk-adverse environments limit development of needed skills such as risk-assessment, adaptation, and resilience, thus affecting aspects of maturity and placing limitations on individuals to learn to recognise and evaluate risks in order to seize opportunities (Livingstone & Smith, 2014). However, literature supports the need for developing specific and general skills and characteristics, that may enable younger people to make considered choices and take evaluated risks both offline and online, in relation to the inter-connectedness of these contexts. This is particularly so if they are to develop a 'concern' for privacy, which is a key determinant in the degree of online disclosure (Liu et al., 2013), and in turn, is

affiliated with negative encounters and risks online. This task falls primarily on caregivers, schools, and organisations with invested interests in the welfare of young people.

Caregivers are parenting in challenging and opportunistic times, however the consequences of the often ubiquitous access many younger children have to digital devices is unknown at this point in time (EU Kids Online, 2014). Therefore, collaborative and integrated approaches are needed to support young people in acquiring the skills and attitudes required to develop into confident, autonomous, and contributing adults.

The following sub-sections review the literature that examines the roles of those who have responsibilities for young people's positive development in relation to privacy concern, and its inter-connectedness with their online experiences.

4.1 The Role of Caregivers

Caregivers are tasked with protecting their children from harm, while also creating safe environments whereby children can learn to take risks, consider consequences, adapt in failure, learn to trust and be trusted. Comparisons made to caregivers' childhood summons considerable differences, and while many caregivers are aware of some of the risks and concerns young people face online, caregivers report feeling overwhelmed and unskilled in finding a balance between trusting and protecting their children in this digital environment (Buckingham & Willett, 2013). Caregivers may lack technical knowledge, or understand little of the new forms of socialisation online for young people, or recognise that young people's identities are formed across offline *and* online contexts (O'Keeffe & Clarke-Pearson, 2011). That so many underage children are on SNSs, and numbers are increasing (EU Kids Online, 2014; Hart Research Associates, 2015), brings into question the degree caregivers are aware and unconcerned (Strom & Strom, 2012). Interestingly, in one report, over half of a large number of parents surveyed confirmed they had allowed their child to create a SNS profile when they were 12 years of age or younger (Hart Research Associates, 2015).

Caregivers are “caught in the middle” (Livingstone et al., 2013, p. 315) in ensuring their child is included with their peer group, even with the knowledge they are underage on SNSs designed for more mature users. Fabrication of information is problematic, and falsified information is used to grant access for underage users, to the services of age restricted SNSs/Apps. Ethics related to ‘lying’ are an important consideration and caregivers who allow their underage child to create profiles, are advised to emphasise ‘safety’ as the underlying motivation for not disclosing all ‘truthful’ information (O’Keeffe & Clarke-Pearson, 2011). Moral and ethical complexities surface in relation to fabrication of information, irrespective of motivations.

Where caregivers were once encouraged to trust their child, the advent of ‘disruptive’ technologies such as the Internet and mobile technologies, and children’s use of these, has seen a shift towards safeguarding and monitoring children’s online activities with greater scrutiny in the home. This could be considered an invasion of children’s privacy even with the best of caregiver intentions. A focus on the rights of children to privacy, and consideration of more democratic parent-child trust based relationships, particularly of older children and teens is encouraged (Buckingham & Willett, 2013; Shmuell & Blecher-Prigat, 2011). Unless there is a concern for the physical or emotional safety from negative influences, Ginsberg (2014) advocates for privacy to be afforded to children, as children need to be trusted in order to learn what trust is.

4.1.2 Caregiver Oversight and Mediation Measures

Caregivers are advised to stay updated with technologies, to ascertain why age restrictions are applied to many SNSs, and have awareness of activities their children are participating in (O’Keeffe & Clarke-Pearson, 2011). While some caregivers were active in talking with their children, connecting to their online profiles, and navigating privacy settings alongside their child, the most prevalent measures undertaken were types of caregiver control such as restricting time, or sites (Madden, Cortesi, Gasser, Lenhart, & Duggan, 2012). As some young people are adept at evading, masking, or obstructing caregiver involvement or

knowledge of their online pursuits, the task of supporting and guiding young people becomes an on-going challenge with caregivers and young people at polar ends of “an externally generated problem – a risky technology” (Buckingham & Willett, 2013. p. 106). Actions such as hiding online content from caregivers, masking screens when caregivers are nearby, deleting History or Cookies, using private browsers, having multiple profiles on SNSs, and even disabling any monitoring software are examples of strategies some young people employ (Cox Communications, 2014). Those who spend more time online, are more likely to learn more digital skills, social competencies, and resilience, though potential encounters with risks online also increase with prevalence of use (Livingstone, 2014; Lwin et al., 2012). However, caregivers can provide crucial channels to increase young people’s knowledge of “privacy-protection and risk-reducing behaviours” (Liu, Ang, & Lwin, 2013. p. 636).

Other studies have explored what types of caregiver mediation are more effective and where both active and restrictive mediation strategies are employed, children are more likely to show greater care over disclosure and protection of their online content (EU Kids Online, 2014; Lwin, Stanaland, & Miyazaki, 2008). Restrictive mediation includes measures such as deciding for the child what they can participate in or view, filtering, monitoring, and/or linking to their child’s online profiles, and are more effectual than no measures at all, but only to younger children (Livingstone et al., 2013). Furthermore, depending on the age of the child, restrictive measures may cause some young people to adopt defensive counter measures to establish privacy boundaries, therefore the more participatory the mediation is, the more beneficial it becomes for both child and caregiver (Schofield Clark, 2011). Active mediation involves discussion between caregiver and child of online content or activities being viewed or undertaken at the time, and are more likely to have a positive influence on privacy behaviours such as disclosure online (Liu et al., 2013; Lwin et al., 2008). Conversely, more permissive parenting styles resulted in greater disclosure online by their children, according to Lwin et al. (2008). However, other obstacles may impact on mediation efforts, for example, the geographical layout of a house in relation to

where devices are used, time availability, or philosophical views in “striking the right balance” between protecting their child, and enabling them access to online environments in light of potential benefits (Ofcom, 2015, p. 37).

In particular, participatory mediation is considered to be the most effectual but requires caregivers to spend regular and sustained time engaged in the technology alongside their child, through actively discussing, co-using, creating, and using the media in meaningful ways *with* their child (Schofield Clark, 2011; Yardi & Bruckman, 2011). This approach encompasses the social, emotional, and cognitive interactions between child and caregiver, changing the perception of authority and autonomy, and is more likely to meet the respective needs of both parties (Yardi & Bruckman, 2011). As both engage in using the technology meaningfully together, there is the potential for discussion to arise over the benefits and risks associated with the online environment. However, Schofield Clark (2011) challenges caregivers’ availability to spend time playing with their children and learning from them in mediated environments. This in turn, raises tension between the literature that supports participatory mediation, and questions whether these measures can be facilitated by busy caregivers, or those with relaxed attitudes towards the technologies and their child’s use of these.

Differentiation is made by Valcke, Bonte, De Weave and Rots (2010) on types of parenting styles that influence young people’s online usage, attitudes and experiences, claiming that those who parent with control and warmth are more likely to have a positive attitude towards technologies, and actively support their children in their online pursuits. In line with these claims, those caregivers who are more technically literate with digital technologies, or who have younger children, or hold concern over the safety and privacy of their child online, are more likely to use filtering and/or monitoring software. However, these restrictive strategies did not result in a reduction of online risks (EU Kids Online, 2014). There is some consensus that measures are most effective when trust, caregiver participation, educational instruction, and some restrictive measures are in place to support children and preteen as they develop conceptual maturity (Liu et al., 2013; Livingstone, 2014; Lwin et al., 2008; Yan, 2009).

4.2 The Role of Schools

Children and teens are often required to work on devices and the Internet which serve as learning tools in the school environment. Therefore, it could be argued that responsibilities and opportunities lie with schools to develop in students, both technical and social competencies in using this online environment. Schools in New Zealand are tasked with ensuring students' physical and emotional wellbeing is protected (Ministry of Education, 2015), and by implication schools now deal with issues occurring online and out of school hours, but spill over into the school environment (Green et al., 2013).

Curricula in some countries include sustained and planned lessons that cover digital citizenship, safety, and media literacies across year levels, however, others struggle to address these areas of need as the curriculum is at capacity and some schools seek other ways to include 'media literacies' into current learning areas (Hague & Payton, 2010; Ontario Ministry of Education, 2015). New Zealand schools are provided with a framework they may choose to use, to help guide their vision and planning of e-Learning which includes aspects of digital citizenship and e-Safety (Ministry of Education, 2010). However, this is problematic, as a 'framework' does not necessarily provide an equitable system for all students in New Zealand. The framework is reliant upon optional uptake by individual schools and staff, and systems of accountability for coverage of these areas of need are yet to be developed. Furthermore, provision of media-literacy learning opportunities may or may not be sustained, nor incremental in coverage and complexity for all students. The effectiveness of programmes undertaken in New Zealand schools is unknown, however research shows that young people enjoy opportunities to learn and engage with cyber-related resources in the context of the classroom (Cranmer, Selwyn, & Potter, 2009; McDonald-Brown, 2012).

The relationship between knowing how the Internet and technologies operate, and the social understandings that underpin safe online behaviour, is "unilateral and asymmetrical" (Yan, 2006, p. 427). Therefore, it is critical that young people are given opportunities to develop "scientific" (Yan, 2006, p. 427) understandings of

these tools, to increase familiarity with cautions and options online (Livingstone & Smith, 2014; Yan, 2009). The concept of ‘e-Safety’ and understandings of what are potential risks, are poorly understood by some children (Cranmer et al., 2009). Education that incorporates learning opportunities of what constitutes online risks, privacy management, and online security, are recommended (Cranmer et al., 2009). ‘Character education’ or life skills, are more authentic learning spheres that adopt the view that ones’ life is a *single* domain which includes both offline and online contexts (Ohler, 2012). Education programs are more likely to succeed in growing the skills and attitudes needed if they include current technologies as learning tools, relational skills, and the values important to localized communities (Ohler, 2012). This approach advocates for students to become familiar with the opportunities and responsibilities accompanying technologies, that they might not only be users of the tools, but question the application of them in partnership with their own values (Ohler, 2012). Few studies have looked into the effectiveness of e-Safety programmes and resources, but current indications suggest content, frequency, allocation of time within curricula, and objectives are disparate and potentially ineffective (Jones, Mitchell, & Walsh, 2013; Milosevic, 2015). This suggests that further research is critical in this area of enquiry.

Further use of the online tools and social spaces young people use online could be integrated in learning programmes (Ito et al., 2008), however this requires pedagogical knowledge in working with new media in learning environments, and affording greater agency to young people in their learning. Conversely, complexities arise in relation to privacy and ownership of content of students’ learning which is often ‘cloud-stored’. There is a growing expectation, and initiative by schools and organisations, for students to upload their learning, assessment, and work to online sites that may allow access for wider public audiences, or dissemination of their personal data (Haduong et al., 2015). Children’s right to privacy of their online learning content needs to be a point of discussion, for stakeholders *and* students. Further research into aspects of

professional development, resources, effective programmes, and student perspectives is recommended to understand needs, risks, options, and solutions in this evolving area of learning and teaching (Finkelhor, 2014; Jones et al., 2013).

4.3 Other Organisations

Yan (2009) outlined the need for quality resources and explicit learning opportunities whereby young people can learn why caution is necessary, measures one can undertake to protect one's safety and security, and skills in dealing with negative encounters. Today, a wealth of Internet safety-related content and intervention material is available online, and is intentionally designed to inform and advise young people and caregivers how to safely navigate social and technical complexities online, and why privacy and security matter. Various sites use multi-media resources that illustrate steps to maintain integrity online, and impart skills to deal with confronting situations when they arise (Common Sense Media, 2015; London School of Economics, 2015). Use of intervention programmes and online resources appear to have some effect in empowering young people (Meter & Bauman, 2015). These are designed to support young people in taking appropriate steps to maintain positive experiences online, and fostering greater understanding of cautions needed in this virtual space (Meter & Bauman, 2015).

In contrast, literature challenges the effectiveness and basis of resources, programmes, and personnel dedicated to Internet safety, security, and citizenship (Finkelhor, 2014; Jones et al., 2013; Livingstone & Smith, 2014). These studies and commentaries purport that the advocacy of types of e-Safety measures prevalent in programmes and resources are not substantiated by robust research and data, and primarily founded on the view that online risks equates to harm, and as yet, are not verifiable through sufficient reliable measures. Sustained learning opportunities are more likely to have impact when compared to 'one-off' sessions by personnel such as police (Jones et al., 2013). Threading crucial messages of managing self online into broader contexts relevant to

both online and offline contexts is more likely to hold rigor, according to a recent summary of Internet child safety materials used by a large task force agency (Jones et al., 2013).

Policy and regulation are the gatekeepers on what actual measures Internet providers and content developers have to meet in relation to terms of use, privacy, and security of users' information and content. Policy pertaining to these need to be informed by robust and reliable research to ascertain what measures are more effective in aiding, empowering and protecting young people in managing risks and privacy, and enhancing social and educational opportunities (Finkelhor, 2014; Jones et al., 2013; Livingstone et al., 2013). Furthermore, maintaining age restrictions of SNSs despite public calls to de-regulate these, and strong endorsement of delaying underage children access to age restricted sites, is recommended (Livingstone et al., 2013). The notion that a self-regulated environment would better serve the wider public interest, and that any regulation ought to be the responsibility of caregivers or persons themselves, is argued against in the current milieu, as "policy should require providers to strengthen current child protection" (Livingstone, Ólafsson, & Staksrud, 2013, p. 318).

4.4 The Agency of Young People

Young people are a crucial resource, as they carry influence within peer groups and are most familiar with what is relevant and affecting to youth. This suggests that the agency of young people may be an effective means of support as youth grow and develop literacies and competencies in new media, and social understandings that accompany these online spaces and tools. Increasing the involvement of "the learner voice" (Cranmer et al., 2009, p. 141) in the development of programmes addressing e-Safety, media literacies, and digital citizenship, is recommended. This in turn, may shape the effectiveness and relevancy of programmes through changing the focus of learning to being "done *by* pupils rather than solely done *to* pupils" (Cranmer et al., 2009, p. 141).

Similarly, when undertaking research in this particular area of online issues, seeking the agency of young people to share their perspectives is strongly recommended, especially to provide an authentic voice to those who make policy and regulation decisions affecting young people (Livingstone, 2013; Livingstone et al., 2014). An example of youth agency can be seen in the organisation ‘Sticks’n’stones’ whose website slogan reads, “Young people taking the lead in promoting positive action online” (Sticks’n’stones, 2016). This New Zealand organisation is run by youth who have banded together to address issues occurring in the online space, after experiencing first hand the difficulties encountered in this online environment, after the loss of friends.

5. Summary

The literature review explored preteens’ concepts of privacy, the degree with which it is valued, and how it may have developed. In addition, any relationship(s) between preteens’ privacy concepts and their interactions with digital devices, and online social environments, were examined. The literature reviewed in this chapter indicated privacy to be complex and difficult to define, however there appears to be some consensus that privacy has types and functions, is a socially negotiated activity, and influenced by cultural factors. It is also an integral aspect of self identity, and woven into aspects of the cognitive, social, emotional, spiritual, physical and moral development of self.

There is a scarcity of literature and studies relating to privacy and young people in *offline* contexts, and existing literature has largely been based on the assumptions of adults. However, laws and policies of many (but not all) countries, uphold that privacy is a child’s right, and legal protection from harm and unwanted scrutiny is provided. More over, in some countries such as New Zealand, laws and policies may also encompass aspects of privacy rights and freedom from harm in online contexts. In contrast, there is a growing body of research and literature related to young people and privacy in the online context. The literature suggests that many online social environments that are co-shared with adult users, pose complex issues for younger users to navigate aspects of privacy control, in both the

technical knowledge and skills, and the social understandings and nuances of these social network sites. The numbers of young people participating on SNSs/Apps and who are under the age requirement is increasing. Similarly, numbers of younger people who have access to mobile Internet-connected devices is increasing, however, implications of these trends are not yet known.

Literature affirms the need for various stakeholders to provide age-appropriate and sustained support to young people, in relation to their online activities and behaviours. Support from caregivers, schools, and agencies is recommended in order for young people to develop the technical skills, social understandings, as well as character traits such as resilience and adaptability required to manage privacy, safety, and security aspects. A wide body of literature indicates the nature of any mediation and oversight employed by caregivers is important, in relation to the effectiveness of supporting, as opposed to censoring young people's online lives. While media and other literature may at times summon public panic in relation to potential risks encountered online, more recent literature is challenging the assumptions that online risks equates to harm, and opposes over-reactions that lean towards a risk-adverse society.

Finally, in response to the scarcity of literature relating to young people and their privacy concepts across offline contexts, I recommended that further research be undertaken, drawing from young people themselves as experts of their own knowledge and concepts. Additionally, the agency of young people in the design of resources, and policies, may be a highly effectual proposition.

The next chapter outlines the design of the research and the theoretical underpinnings for this study.

Chapter Three: The Research Design

Introduction

The research design for this study is outlined, beginning with the research question in section one. The following two sections describe the theoretical perspective of the researcher, and the interpretive paradigm in which the study is positioned. A qualitative approach to data collection was adopted, and is discussed in section four, while the research methods and instruments which include the design of the survey, selection of participants, and administration of the survey, are detailed in the fifth section. The management of ethical considerations, access and acceptance of the study, the nature of informed consent and confidentiality, and due care taken in relation to any potential harm, are discussed in section six. Issues of validity and trustworthiness are the focus of discussion in section seven, and the coding and analysis processes are described in section eight, with examples shown in Table 1. The chapter concludes with a brief summary.

1. The Research Questions

As discussed in Chapter One, the principal research questions were:

What are preteens' concepts of privacy and how might these have developed?

How do these concepts relate to their actions and decisions in online social environments and with digital devices?

2. Theoretical Position

How one sees the world, that is, one's beliefs about truth and reality, can influence the ontological and epistemological positioning of research, which in turn, may shape the lens through which reality or phenomena is perceived and acted upon (Cohen, Manion, & Morrison, 2011). Ontology refers to how one

perceives reality, the beliefs of what exists in the world (Davidson & Tolich, 2003). Ontology seeks to understand ‘what’ and ‘why’ a particular thing occurs and how it relates to other things. In this study, a subjectivist ontology is assumed, that is, the concern or interest in ‘being’ is relative, and realities are both local and specific and at times co-constructed (Lincoln, Lynham, & Guba, 2005). In relation to this study, such a stance assumes each preteen participant will have their own views and perspectives in relation to the world around them, and therefore their own interpretation of experiences related to privacy, devices, and participation on online social networks, and how this is valued.

Epistemology relates to the nature and form of knowledge, and is concerned with how knowledge is procured and shared (Cohen et al., 2011). It is concerned with the natural sources, scope and limits of knowledge, and seeks to discover meaning. The subjective epistemology recognises that the world can be perceived in different ways, and accommodates these differences (Cohen et al., 2011). In adopting a subjective epistemology, I believe that participants’ knowledge is unique, subjective, and socially constructed, that is, what they believe to be knowledge is the result of a complex interaction of variables specific to their context and situation. Therefore, as the researcher, I argue that participants bring to this enquiry individual and valid understandings built on their social interactions and experiences, thus providing an opportunity to look into the significance of participants’ individual knowledge, in relation to their views of privacy and confidentiality, and how this plays out in online environments.

This leads to the next section, which discusses the interpretive paradigm that is aligned with this study.

3. An Interpretive Paradigm

The adoption of an interpretive paradigm, while acknowledging its epistemological subjectivity, is most suited to understand the participants’ own experiences and perceptions as they reported these, being ‘experts’ of their own thoughts and feelings (Burke, 2005; Clark & Moss, 2011). The intent in eliciting

preteens' 'voice' in this study was to better understand their perspective, adopting the belief that they were 'most suited' to report their concepts and experiences. Furthermore, the interpretive paradigm argues that the "social world can be understood only from the standpoint of the individuals who are part of the action" (Cohen, Manion, & Morrison, 2007, p. 19), confirming the appropriateness in the first instance of seeking participants' perspectives in relation to the focus of this research.

An interpretive paradigm begins with participants' reports and uses findings as the basis for any latter hypothesising or possible theorising. This is in contrast to the positivist paradigm that frequently originates with a hypothesis that is subsequently tested to support, refute, or create theories (Lincoln et al., 2005). The subjectivist positioning adopted by this study sought to understand participants' worlds as they perceived them, using methods of data-collection that supported this in a trustworthy and transparent manner.

4. A Qualitative Approach

When planning research, the concept of 'fitness of purpose' is critical, in that the focus of the research determines the design and methods used (Cohen et al., 2011). Additionally, when the intention of the research is well-defined, the best methods for fulfilling the research goals can be established (Mutch, 2013).

When seeking a deeper understanding of children and their social and cultural lives, as was the purpose of this enquiry, it is probable that a qualitative approach to research is adopted (Tinson, 2009). The study sought insights and understandings of particular preteen behaviours and concepts, therefore a survey method was selected and undertaken to support the research goal, using open short response questions as the starting point. Particularisation of the findings to the preteen sample in this study aligned with the adoption of a qualitative approach, rather than seeking generalisations applicable to all preteen children, where a quantitative approach using a survey of a very different design with a larger sample, may have been more suited.

5. Research Methods and Instruments

This section describes the survey method used, the design of the online survey, and the processes involved in selecting the participants. The management and processes of the survey are also discussed.

5.1 Research Methods

A focus group was undertaken as well a short response/Likert scale/multi-choice survey, thus adopting a mixed-methods approach. The responses from the survey provided an abundance of “rich and thick” data (Cohen et al., 2011, p. 183) of sufficient depth and scope for the purposes of this study, therefore analysis of the focus group data and its subsequent reporting and discussion will be undertaken for other publication purposes.

5.1.1 Survey

A web-based, group-administered survey was selected as the key data-gathering instrument to source qualitative data at a single point in time. This particular data-gathering method can provide an expeditious means to gather information from a selected population in a “single ‘pass’ through” (Sapsford, 2007, p. 17). The selection of the survey method potentially enabled a large group of preteens (60), to share their perspectives, concepts, and experiences in an expedient and comprehensive way. A web-based survey also offered the benefit of results being reported directly into a database almost immediately at the conclusion of the survey, thus avoiding any potential inaccuracies or bias through the researcher entering data on behalf of participants (Cohen et al., 2011). The survey was conducted in each school separately in one ‘sitting’, at a time that suited the particular school’s calendar, schedule, and supervising teachers’ requirements, and all were completed within a seven-day period.

5.1.2 Survey Design

The survey contained 30 items and included open and closed questions - Likert scales, matrix questions, multi-choice and single-choice options (Appendix A). Some questions sought qualitative responses in which participants reported their perceptions and experiences. Certain questions required only a click of the mouse to select the response most aligned to participants' experience or perspective, while others sought more lengthy descriptions in participants' own words, and some questions sought responses only if participants wished. Careful consideration was needed in the structure of sentences, words, terminology and instructions used in the survey, to ensure readability and comprehension for this particular age group (Cohen et al., 2011). The design of the survey included considerations of font clarity, arrangement of the order of questions so that participants did not tire of typing their own responses, and maintaining a flow of topic within the arrangement of questions.

The survey was structured into two main sections, the first concentrating on the broad concepts of privacy and privacy importance, how these may have developed, and what, or who may have influenced these. The second section focused initially on digital devices, awareness of age restrictions on SNSs/Apps, participation in SNSs/Apps, and caregiver oversight. Subsequent questions looked into privacy aspects of SNSs/Apps, issues related to contact, conduct and concerns, and perceptions of competency in managing privacy online. A rubric of the questions was constructed to ensure coverage of the key areas of research enquiry (Appendix B). It is strongly recommended to pretest a questionnaire/survey with younger people as their cognitive, memory and linguistic skills are still developing (Carson, 2007). While a pilot trial was planned, due to the unforeseen clash of commitments for five students scheduled to undertake the pilot, it was not possible to execute this in time, prior to the first scheduled survey administration. However, survey questions had been carefully considered by a peer educator and the research supervisor for bias, length,

accuracy of what was intended to be measured, usability, and type of data that might be gathered. This led to a select few questions being omitted or re-phrased for further clarity.

5.1.3. Selection of Participants

Those surveyed must accurately represent the population being represented so that validity of the sample is established in the research (Sapsford, 2007). Therefore, the numbers and make-up of the surveyed sample is an essential element in the design stage of the research method. While the research focus did not include differentiating the data or findings in relation to gender, it was intentional that the make-up of participants would reflect a balance in numbers of females and males from across the three schools. This was planned for so that the data would not be potentially skewed through a possible gender bias. This was achieved with the selection of 20 participants from a ‘boys only’ school, 20 participants from a ‘girls only’ school, and 10 male and 10 female participants from a co-ed school, who met the criteria for participation.

The selection of participants was based on criteria that required participants to be *between* 11 and 13 years of age; have at least one online social network profile; have a reading age similar to their actual age; competency in using a keyboard; and provision of assent to participate in the research. The supervising teacher from each of the schools was tasked with outlining the research proposal and purpose to larger groups of possible candidates who might meet the criteria. Final selections were made on a ‘first in’ basis. More students than the decided number of sixty agreed to undertake the study, which in turn provided a reserve of participants if any unforeseen absences occurred on the day/hour when the survey in each of the participating schools was scheduled.

5.1.4 Management and Process of Survey

Once their supervising teacher confirmed the assenting participants through documentation, a day and time was scheduled for the survey to be undertaken in an allocated room within the school, with a supervising teacher and myself present. As the researcher, I introduced myself at the beginning of the session and briefly outlined the purpose of the research and the nature of the survey, using a standardised script (Appendix C). Participants were briefed on what assent meant, and their rights to withdraw at any time prior to submitting their responses. Participants' rights to confidentiality of information they provided were detailed, as well as the steps of the survey itself and types of questions included. It was also important to emphasise the difference between the survey and school assessments to reassure participants that there was no 'right or wrong' response, but rather, authenticity of responses was most desirable (Check & Schutt, 2012). Each participant was required to access the online survey via a Google Form using a provided link, and this was achieved through either participants' devices or school-owned devices.

Participants undertook the survey, and if support was required in reading a question or clarifying any words, either the supervising teacher or myself approached those who indicated so. This process also served to expose several questions that indicated the need for further explanation for some participants across the three schools. These few occasions where further clarification was sought, had little impact on the data from the survey generally. One hour was allocated to completing the survey, enabling every participant enough time to do so, and responses were confirmed via a 'submit' button. At the conclusion, every participant was thanked for their valuable contribution, reassured of their confidentiality and anonymity, and given a chocolate bar of their choosing for their endeavour. Similarly, each supervising teacher was thanked and acknowledged for their support and effort.

The next section discusses the ethical procedures and guidelines that were adopted for this study.

6. Ethical Procedures

Honesty and transparency underpin any research that adheres to ethical principles, codes, and procedures. Additionally, preservation of the dignity of all those involved through respect and care of their wellbeing and personal rights, are also central (Check & Schutt, 2012; Cohen et al., 2011). Protection of children participating in research is an essential aspect of the research design and particular ethical considerations are required (Lewis & Lindsay, 2000). I was highly sensitive to the nature of working with younger participants, and aware that protection from harm included physical, psychological, social, economic, and cultural aspects, as per the ethical principles expected in this study (Waikato University, 2008). This study, having shown appropriate consideration of necessary consents, assent, and meeting procedural requirements and pastoral understandings needed in research, met the approval from the Ethics Committee of Waikato University in January 2015 (Serial Number EDU 112/14).

6.1 Access and Acceptance

Access to participants and acceptance of the research is required by an organisation and individuals where the study will be undertaken, prior to its commencement (Cohen et al., 2011). Where the researcher is a member of the organisation, or known to the organisation(s), this can help minimize barriers or problems (Cohen et al., 2011). As the participating schools' management personnel knew me in some capacity as a local educator, a degree of credibility was established early on, and was further supported through meeting the appropriate ethical and procedural requirements and communicating to all those involved, the detail of the research and methodology to be undertaken.

6.2 Informed Consent, Assent and Confidentiality

In undertaking research with children, ethical codes and guidelines have been established to ensure the safety of those participating, as well as the confidentiality and security of information they provide for the purposes of the research (Lewis & Lindsay, 2000). For this study, the ethical code and guidelines that were followed were sourced from the University of Waikato Ethical Conduct in Human Research and Related Activities Regulations (Waikato University, 2008). The caregivers of those who indicated an interest in participating were sent an email that contained an overview of the study (Appendix D), and an information sheet and consent form (Appendix E). Confirmation and informed consent from caregivers was compiled by way of emails, Google doc forms, and hard copies sent to the coordinating teacher, and then on-sent to myself, with all communications confirming consent stored securely and appropriately. When working with younger participants, assent is required in addition to caregiver consent, and participants must be given the opportunity to assess voluntary participation in relation to the information provided (Tinson, 2009). The nature of assent was verbally explained at the introduction of the survey. Similarly, participants were briefed on their right to withdraw at any time during the survey, and needed only to indicate so to the supervising teacher or myself. A standardised script (Appendix C) was used during the introduction that detailed what assent was, and rights of withdrawal, and emphasised that by activating the 'submit' button at the end of the survey, assent was confirmed. These actions signaled an acknowledgement of their willingness to voluntarily participate in the study.

Heads of Schools and supervising teachers were also required to provide confirmation of informed consent, and were provided with an appropriate letter and consent form (Appendix F). This form outlined the responsibility of the Head of School to inform the respective Board of Trustees and gain the appropriate permissions. Additionally, they were responsible for any decisions to report to the wider school community the news of involvement of some students in the research study, if need be.

Confidentiality is assured but not guaranteed, and circumstances may at times require overriding aspects of confidentiality if participants' wellbeing and/or safety could be endangered through circumstances that may potentially or actually cause harm. The ethical principles in such situations require the researcher to commit to "respect for the dignity of the persons, responsible caring, integrity in relationships, and responsibility to society" (Lewis & Lindsay, 2000, p. 18). In this study the researcher's brief included guidelines that outlined the confidentiality of responses, as well as anonymity of any identifying information such as names and email addresses (enabled through use of the Google Form). It was emphasised that no individual's responses would be disclosed, and that the storage of their responses would be secure. Participants were invited to question any aspect of the confidential and anonymous nature of the survey and any personally identifying information, prior to commencing the survey.

6.3 Harm

Mitigating any possible harm to participants that may arise as a result of particular questions, or the process of participation itself, were of importance (Cohen et al., 2011; Tinson, 2009). Observing participants as they worked through the survey, responding to any questions, and debriefing at the end of the survey were strategies of reflexivity undertaken by myself as the researcher. I had prepared appropriate actions to be undertaken in the event of any participant withdrawal, or in the event of any disclosure by a participant that raised any concern for their wellbeing. While I did not know the name or email of any participant, I was able to ascertain the school, due to the Google Doc spreadsheet indicating a date on which the survey had been submitted. These ethical protocols were essential, as one situation of concern arose from a particular response to a short answer question, and further steps were required. The particular school and supervising teacher were contacted and thoroughly briefed on the issue relating to the disclosure. The discussion produced assurance that an appropriate course of action would be undertaken for those involved. The particular case is discussed further in the Findings chapter.

7. Validity and Trustworthiness

This section considers issues of validity and trustworthiness. In order for readers of a study to trust the research outcomes, they must have confidence that the processes and findings that emerge from them, are robust (Mutch, 2013). This was the aim in this study, and was sought through adopting transparency, adherence to ethical procedures, and clarity and detail in the documentation of the methods used and approaches to data coding and analysis.

The research ‘problem’ must be well-defined according to Sapsford (2007), in order for a survey to hold validity, measuring accurately what is suppose to be measured with some consistency and accuracy. Simply, validity is “the degree of correspondence between a measure and what is measured” (Fowler, 1998, p. 371). The data elicited and reported in this study provided depth and scope in the examination and exploration of participants’ understandings and experiences. Considerable detail has been provided through the “rich and thick” (Cohen et al., 2011, p. 183) data elicited from participants, as presented in the Findings. Many examples of the qualitative data are shown in tables in the Findings to “support and corroborate findings” (Cohen et al., 2011, p. 183). Thus, the validity and trustworthiness of the findings and outcomes reported, are strongly supported through the depth and detail of reporting.

As this enquiry was subjective in nature trustworthiness was a goal, that is, data interpretation provides an accurate representation of participants’ views and reports. In this sense the study reported the responses to questions from the perspectives and vantage point of each individual, in that data representation “represents the perspective of the child, whether of a particular time, or a more permanent attitude” (Lewis & Lindsay, 2000, p. 194). As there is “no basis for determining that one perspective is the ‘valid’ one” (Check & Schutt, 2012, p. 39), this infers all perspectives are valid, based on participants’ perceptions of reality, and ‘how it is for them’. Therefore, as the researcher it was important that all responses were fully and appropriately considered, and where responses

reflected an alternate or ‘outlier’ perspective or experience, this was reported accurately. An example of this was one participant’s voluntary response that indicated they had engaged in a form of self-harm at one point in the past, as a result of encountering online bullying. This is further discussed in the section on harm in this chapter.

Cohen et.al (2007, p. 134) describes validity as “the meaning that subjects give to data and inferences drawn from the data that are important”. This places importance on the reliability of reporting by the researcher, to ensure that the “factual accuracy of the account is not made up, selective or distorted” (Cohen et al., 2007, p. 134). The challenge for myself as the researcher lies in my ability to understand and interpret the meaning and intent of participants’ responses and minimize any bias I might bring to the study, thus maintaining the interpretive validity of the study. Attention has been given to ensure transparency and accuracy in the representation of participants’ information in this study, and many examples have been provided in tables in the Findings to support the trustworthiness of any interpretations made from the data.

The next section discusses challenges to the validity and trustworthiness of the study.

7.1 Challenges to Validity and Trustworthiness

When endeavouring to measure concepts, perceptions, and attitudes, there is the potential for ambiguity to arise, particularly in the stages of analysing and interpreting responses. To help minimize any potential ambiguity during the stages of analysing and interpreting responses, I sought to use consistent and authentic processes that “reflects fairly the various perspectives of participants in that setting” (Check & Schutt, 2012, p. 39).

The findings may have been influenced by limitations in participants' responses as a result of 'how they felt' on the day of the survey, and raise the question whether the 'snapshot' of their concepts of privacy and online activities accurately reflected their actual ideas, activities and behaviours (Tinson, 2009). Similarly, the personality of a participant may influence the approach one may take to answering open-ended questions, potentially producing some responses with longer descriptions, and others with minimal descriptions. These 'participant' factors needed to be considered carefully in the coding and analysis stage of the study to maintain aspects of validity, as some participants provided lengthy responses, and others were minimal. Furthermore, this aspect did not appear to be influenced by gender.

Poorly worded questionnaires that can "inhibit or truncate the child's full and necessary expression" (Lewis & Lindsay, 2000, p. 194) may potentially affect the design validity. In addition, the researcher must accommodate the developmental status of the younger participants irrespective of the soundness of method selected, to ensure aspects of validity are considered, and strategies to meet potential challenges are in place. While I endeavoured to check for clarity in the wording of questions taking into account reading age and comprehension, two questions required further explanation for a number of participants in the sitting of the survey.

8. Data Coding and Content Analysis

All survey data gathered were collated on a Google Doc spreadsheet, and charted. The deeper coding and analysis of qualitative data required a methodical and organised approach to categorize and explain participants' descriptions and explanations, to identify patterns or themes (Cohen et al., 2011).

In the initial stage, I undertook a familiarisation exercise to help me become familiar with the “range and diversity” (Tinson, 2009, p. 134) of the data. I used an inductive approach to derive individual themes from the data, from which an initial sweep of meaning could be drawn. A thematic framework was then created, providing a structure for categorizing descriptions in the data during the initial analysis and coding. In the second stage, the assigned themes were re-examined, and emergent themes and categories established with greater rigor. In the third stage, previous iterations of the coded and categorized data were further scrutinised before tabulating and quantifying the data by type and frequency, then representing the data in tables. At this stage, I was able to explore any associations between the data sets, in line with the original research question. Key characteristics were drawn together and interpretations of the overall data were made. It was important to confine any associations to the actual data, and where possible, this was undertaken.

I worked not from any preconceived theories or researcher assumptions, but from participants’ direct experiences and ideas, as those were most expertly situated to provide insights into their world (Burke, 2005; Clark & Moss, 2011).

The table below contains an example of the coding process applied to the qualitative data, and how descriptive labels and themes emerged.

Table 1.
Summary Example of the Coding Process with Qualitative Data

Example of the Coding Process Relating to Question 3 of the Survey:

Question 3. What is 'privacy' or 'having privacy'?

Example One

“Privacy or having privacy is when you have a right to your own information and no one is allowed to access it” (Participant #9)

Stage 1. Familiarisation.

Three descriptive labels/themes were evident when interpreting the above response. Firstly, ones' *rights*; secondly, *control*, and thirdly, *personal information*. Three comments were counted due to three separate ideas being conveyed. The use of the word 'rights' was interpreted as an indication of awareness of autonomy and individualism. The second comment relating to access, was interpreted as control of boundaries regarding others' access. The third comment refers to 'own information', and was therefore labeled as '*Personal Information*'. The first two comments or ideas were closely related but still distinctive, and were labelled as '*Autonomy and Control*'.

Stage 2. Thematic Framework.

Once familiarized with all participants' data in Stage 1, I reviewed each response again looking closely at the themes that had emerged across the data during earlier iterations. I re-checked each response in accordance with early emergent themes, and ensured I had been as authentic and consistent in the analysis process, and made any necessary changes to the analysis process during Stage 2.

Stage 3. Rigorous Scrutiny and Tabulation of Data.

After working through Stages 1 and 2 with participants' data relating to this question, it became clear that eight categories emerged from the thematic analysis. These were *Autonomy and Control*; *Personal Information and Confidentiality*; *Personal Space and Solitude*; *Personal Belongings*; *Relationships and Trust*; *Physical Body and Physical Safety and Security*. In analysing these, it was evident these could be further labelled under three dimensions relating to 'self'. These are the Personal Self, the Social Self, and Physical Self. The eight categories and dimensions of self are shown below Example Two.

Example Two

“No one else is there. By your self. Keeping everything to your self so no one else knows or can see what you are doing. Privacy is something that everyone has the right to have. Being able to share your thoughts/feelings with someone without them telling anyone else. People need to respect your privacy” (Participant #51)

Stage 1. The fullstops indicated separate comments and totalled 6. The response was coded as follows:

“No one else is there **(Personal Space)**. By your self. **(Solitude)** Keeping everything to your self so no one else knows or can see what you are doing **(Control)**. Privacy is something that everyone has the right to have. **(Autonomy)** Being able to share your thoughts/feelings with someone without them telling anyone else. **(Relationships and Trust)** People need to respect your privacy **(Relationships and Trust)**”

The first two comments emphasise space and solitude as aspects of privacy. The third comment indicated the role of autonomous decisions relating to boundaries and access. The fourth comment reflected personal rights. The fifth comment indicated relationships and trust were important. The last comment indicated that relationships involve respect in relation to privacy.

Stage 2. After carefully reviewing the six comments in the second stage of the process, these were then tabulated under the categories of Personal Space and Solitude (x2), Autonomy and Control (x2), Relationships and Trust (x2).

The themes that were created, were formed largely by the recurrence of similar data from multiple participants, however, when there were only a few reporting an alternative aspect,

this was appropriated to its own theme, as opposed to any data being misrepresented or manipulated. This was seen in the few comments aligned with physical safety and security.

Stage 3. When the six themes were considered in relation to all the data from Question 3, it was evident that these related to aspects of self. These were the personal, social and physical self, and became the overlying labels. These are shown below:

PERSONAL SELF

Autonomy and Control; Personal Information and Confidentiality; Personal Belongings;
Personal Space and Solitude

SOCIAL SELF

Relationships and Trust

PHYSICAL SELF

Body, Safety and Security

9. Summary

In summary, this chapter described the theoretical stance and the interpretive paradigm in which this study was situated, and explained its intent to understand viewpoints from the individuals' perspectives, taking into account the particular contexts within which their knowledge and beliefs have been formed. A qualitative research approach was adopted, to understand perspectives from those most expert, that is, the participants themselves. This in turn, influenced the selection of a survey tool for the purpose of gathering qualitative data from a large number of participants.

The design of the survey, the selection of participants, and administration of the survey were described, including particular considerations required when working with younger participants. Ethical responsibilities and procedures that were adopted were outlined and included informed consent and assent, participants' rights, confidentiality, and strategies for the protection of participants' wellbeing and safety. This chapter also described issues of validity and trustworthiness, and detailed how any potential issues that could have arisen were dealt with. The last section outlined the processes and stages used in coding the data, and two examples in Table 1 explain these stages, including how themes from the qualitative data emerged and were subsequently labeled.

The following chapter presents the findings of the research that correspond to the themes and dimensions outlined in this section.

Chapter Four: Findings

Introduction

The findings from this study that inquired into participants' privacy concepts and practices, and any association(s) to their online actions and decisions, are shared in this chapter and organised in five sections based on specific enquiries. Age and gender of participants are reported in the first section. The second section outlines perceptions, examples, and influences in participants' development of privacy. The third section examines what digital devices and SNSs and Apps participants used online, and in addition, caregivers' mediation or oversight relating to participants' online activities and use of devices. The fourth section outlines participants' experiences, actions, and influences encountered in online environments. The fifth section looks at participants' knowledge and use of online tools and settings that can aid privacy, and explores their competencies in managing online privacy, security, and safety. Quoted data were transcribed verbatim from survey comments. The data elicited from two survey questions generated ambiguous findings and have therefore been omitted from the findings in this chapter. A brief summary concludes the chapter.

1. Demographic Information

Criteria for participation required all participants to be aged between 11 years and under 13 years. 'Active participation', defined as having an account or profile on at least one online SNS/App at the time of involvement in the study, was also a criterion. This factor confirmed participants' activity on SNSs/Apps, many of which carried age restrictions of 13 years and over (13+). This issue is raised in an interesting discussion on underage activity on SNSs/Apps in the preceding chapter. Gender included female (50.0%) and male (50.0%) and the majority of participants (83.0%) were over twelve years but under thirteen years. Age groups and gender of participants are reported in Table 2.

Table 2.
Demographic Data of Survey Participants

Gender and Age (Years)	Percentage of Responses
Female	50.0
Male	50.0
11-12.0	17.0
>12 - <13	83.0

Note: N=60

2. Concepts, Examples, and Influences Related to Privacy

Section Two reports data on participants' broader concepts, examples, and influences related to privacy. I was interested in relationships, if any, in the data whereby similarities and/or differences might be found between concepts of privacy and examples of privacy importance. Where qualitative responses were elicited in some survey questions, these were coded thematically. Data were then categorized using content analysis to organise responses as themes developed. Data are reported in tables.

2.1 What is Privacy?

Participants were asked to describe what privacy is and wide-ranging responses were recorded. A summary of data related to general privacy concepts and examples of privacy importance in participants' lives, is reported in Table 3. The intention was to ascertain trends and specific insights into privacy that might emerge from this group. Their ideas characterized personal, relational, and physical aspects of privacy. This provided an interesting and early premise in relation to survey data and any subsequent associations that might surface.

Of significance was the prevalence of responses in which concepts of control and autonomy featured as aspects of privacy. These were noted in 40.0% of responses. Participants in this group expressed ideas describing one's rights in making decisions affecting them, rights relating to objects and belongings, and

rights of one's self as an entity. Identity was strongly woven in these ideas, and citation examples in Table 3 were selected to illustrate these important aspects. Aspects of control and autonomy were represented in both online and offline contexts indicating the seamless nature of the two worlds in which they take part. In addition, many references were made to one's personal information (P.I) in either offline or online domains. Participants denoted ideas of concealment, protection, and types of P.I in 40.0% of responses. Citation examples in Table 3 reflect privacy concepts representative of this group.

Personal space and solitude were noted as aspects of privacy by a smaller number of participants. Privacy included a physical place to be alone and/or a desire for solitude, as indicated in 10.0% of responses. Also noted were references to possession and/or ownership of belongings. Ownership was indicated in use of 'my' or 'your', and illustrated in the following citation, "Keeping your belongings to yourself" (Survey Respondent #45). Relational aspects and trust as privacy aspects, were evident in 5.0% of participants' responses, with several indicating 'others' such as friends, were trusted to keep certain information 'secret'. A small percentage of participants shared privacy ideas related to one's physical safety, and interestingly, one participant recognised the notion of invasion of privacy, if one was to be 'watched' through a camera (Survey Respondent #54).

In summary, many participants indicated attributes of control, autonomy, P.I, and confidentiality as important aspects of privacy. Of less prominence but also attributed to privacy meaning were aspects of personal space, solitude, relationships, and trust. Only a small number noted aspects of physical safety and personal belongings as integral in privacy. The role of privacy in participants' lives was of interest, and their personal examples of privacy importance are examined in the next section.

The Table below reports categorized qualitative data relating to participants' concepts of what privacy is.

Table 3.
Categorized Comments of Participants' Concepts of Privacy

Categories of Participants' Concepts of What Privacy Is	Percentage of Comments
<p>Control and Autonomy</p> <p><i>Citation examples:</i> ...is something that only you or people that you want are allowed to look at it (Survey Respondent #1); ...being your own person (Survey Respondent #12); ...your ideas and thoughts are left to yourself (Survey Respondent #44) Privacy means to me having full control over my account...(Survey Respondent #13); not letting anyone see things because it is rightfully yours (Survey Respondent #55); ...being able to do something without other people or things viewing it or knowing about it (Survey Respondent #8); ...being able to live your own life (Survey Respondent #12); Being able to act how you like to... (Survey Respondent #54); Privacy is when you are able to do your personal things...without worrying about people surveying you without your own consent (Survey Respondent #45); ...freedom from interference (Survey Respondent #46); I think privacy is having something to yourself ...(Survey Respondent #17)</p>	40.0
<p>Personal Information and Confidentiality</p> <p><i>Citation examples:</i> Secret. For your eyes only (Survey Respondent #21); Random people I don't know seeing my social media profiles (Survey Respondent #3); Privacy is your information and not giving out personal information (Survey Respondent #6); It is not showing your private information/photos with the public (Survey Respondent #13); Privacy is secret in away, to have a personal secrecy (Survey Respondent #57); I would not like other people snooping around my Snapchat...(Survey Respondent #11); Having privacy means to me that my accounts are secure...(Survey Respondent #13); Don't show anyone your passwords (Survey Respondent #59); Knowing your email and stuff like that are safe so noone else can see (Survey Respondent #14); (Survey Respondent #); Your identity is not able to be seen by others that you do not want them to see (Survey Respondent #18); Information you want kept secret (Survey Respondent #24)</p>	40.0

Space and Solitude	10.0
<p><i>Citation examples:</i> ...privacy is having your own space without someone continually watching you or in your personal bubble (Survey Respondent #5); Being in my room by myself reading a book or doing homework so I can actually think and not be distracted... (Survey Respondent #21); When you're alone and no one disturbs you (Survey Respondent #33); It's like having your own room that no one can go into...your own thoughts (Survey Respondent #55); Having your own space (Survey Respondent #52) Privacy is having your own space and people can't look at what you are doing (Survey Respondent #49); Alone time (Survey Respondent #24)</p>	
Belongings	2.0
<p><i>Citation examples:</i> Keeping your belongings to yourself (Survey Respondent #46); Having your own things (Survey Respondent #52); ...have stuff that other people can't go into (Survey Respondent #1)</p>	
Relationships and Trust	5.0
<p><i>Citation examples:</i> Friends telling other people secrets that I didn't give them permission to share (Survey Respondent #3); ...show only who you want to show and expecting them to keep it zipped (Survey Respondent #57); ...only have people I trust looking at my social media pages...(Survey Respondent #3); Being able to share your thoughts and feelings with someone without them telling anyone else (Survey Respondent #52); I'm not too worried about my privacy around people I know...but I don't like secrets or things quite private about me going out into the open...(Survey Respondent #20)</p>	
Physical Body and Physical Safety	2.0
<p><i>Citation examples:</i> ...make sure the doors and main windows are locked so no one can come in and harm me or my family members (Survey Respondent #58); ...if cameras were watching you that would be an invasion of privacy (Survey Respondent #54); Having safety and security...(Survey Respondent #4); Stranger danger (Survey Respondent #46)</p>	

Note: Comments relating to privacy N=267.

2.2 Importance of Privacy in Participants' Lives

The importance of privacy in participants' lives was evident in personal examples, and resulted in a rich collection of data reported in Table 4. Convergence

between participants' personal examples of privacy importance, and concepts of privacy was significant. Many participants provided lists of what comprised P.I, also, many associated aspects of disclosure and/or confidentiality to their P.I. These were evident in 55.0% of comments and examples are presented in Table 4. Some participants simply noted this aspect as "Personal information" (Survey Respondent #55). Numerous examples provided by participants in this group occurred in offline and/or online contexts. Strong views of self and the rights of self underpinned ideas of personal control and autonomy, and were evident in 19.0% of responses. The desire for independence and right to privacy are reflected in citation examples representative of this group and presented in Table 4.

Also noted, was the perception or actual ownership of belongings, and indicated in 6.0% of responses. Several participants referred to online environments, for example "Keeping your belongings and internet life safe" (Survey Respondent #35). Specific physical places or the idea of one's personal space, and/or solitude featured in 9.0% of examples of privacy importance. Citations reflected this aspect of ownership of spaces or places, and are evident in the following examples, "My room" (Survey Respondent #51), and "Having space alone" (Survey Respondent #14).

Relational aspects and trust were important in some participants' personal examples of privacy importance. Participants in this group highlighted the act of entrusting select information to 'others' such as caregivers or friends, as a key aspect of privacy. This was evident in 9.0% of responses and citation examples are presented in Table 4. In addition, examples relating to one's physical safety and body were evident in a small percentage of responses. Protection from "stalkers" was mentioned (Survey Respondent #44) as well as reference to one's "body" (Survey Respondent #6).

In summary, participants' concepts of privacy, and personal examples of privacy importance were expressed as aspects of the personal, relational, and physical self across both offline and/or online contexts. Prevalent aspects of privacy that

emerged were control and autonomy, and P.I and confidentiality. Personal belongings, space and solitude, relationships and trust, physical safety and body were also central in privacy concepts and examples of privacy importance for groups of participants.

The table below reports categorized qualitative data from participants' personal examples of privacy importance in their own lives.

Table 4.
Qualitative Comments Categorized, of Privacy Importance in Participants' Lives

Categories of Privacy Importance	Percentage of Comments
Personal Control and Autonomy <i>Citation examples:</i> ...you want to keep things to yourself (Survey Respondent #27); I can be me...(Survey Respondent #20); Not always having my family knowing every single little detail of my day (Survey Respondent #52); You don't want people to tell/gossip to anyone so you don't tell anyone (Survey Respondent #56); Don't let people go in my room with out my permission (Survey Respondent #59); Not take a photo of you without you agreeing to it (Survey Respondent #18); Things that are going on in my life (Survey Respondent #23); Having some of your own time (Survey Respondent #43)	19.0
Personal Information and Confidentiality <i>Citation examples:</i> People going into my accounts...(Survey Respondent #19); Where I live, name, cell-phone numbers, password in general (Survey Respondent #39); My messages, KIK messages, Snapchat, photos (Survey Respondent #47); Personal information (Survey Respondent #55); When On-line so no randoms can see my profile/ pictures eg (Instagram, Snapchat...) (Survey Respondent #46); Texting, communicating, ringing, social media (Survey Respondent #37); Passwords, profiles and secrets (Survey Respondent #8); they cannot see your email, age or personal information (Survey Respondent #18); Homework..school work (Survey Respondent #22); On my phone (Survey Respondent #28); The stuff on my device...things I only tell my teacher...things I tell my parents... stuff I only want my best friends to know (Survey Respondent #30)	55.0

Personal Belongings	6.0
<i>Citation examples:</i> My belongings (Survey Respondent #22); Keeping your belongings and internet life safe (Survey Respondent #35); ...having my own things (items owned by me) Survey Respondent #26); When I am on my device (Survey Respondent #5); Personal Belongings (Survey Respondent #13); I don't like it when people feel they can go through my stuff without asking...when people go through my phone, I'm not hiding stuff but it is still my phone (Survey Respondent #29)	
Personal Space and Solitude	9.0
<i>Citation examples:</i> ...having space alone (Survey Respondent #15); I want to be alone and private...(Survey Respondent #28); My room (Survey Respondent #51); My bedroom (Survey Respondent #4); Having time alone (Survey Respondent #12); sometimes I need to be in my room by myself so I can think (Survey Respondent #22); Personal space (Survey Respondent #47)	
Relationships and Trust	9.0
<i>Citation examples:</i> Talking to my mum/family (Survey Respondent #34); The stuff that needs to stay in-between my family/family issues (Survey Respondent #42); Things that I tell my best friend (Survey Respondent #48); when I want to chat to my family or friends (Survey Respondent #9); Stuff just between you and someone else not just everyone (Survey Respondent #7); Only me and the person... are allowed to look and if someone else look they're invading my privacy (Survey Respondent #17)	
Physical Body and Physical Safety	2.0
<i>Citation examples:</i> Your body (Survey Respondent #7); Going to the toilet (Survey Respondent #14); Not have people watching you like a stalker on-line and outside of on-line (Survey Respondent #44); Bathroom. Body (Survey Respondent #3); In the bathroom (Survey Respondent #4)	
Note: N=312 (Number of comments).	

2.3 Perceptions of Privacy Importance

Inquiry into participants' perceptions of how important privacy is to them, and comparing their need of privacy to others close to them, was valuable in exploring whether social and/or cultural influences may be factors in the development of their privacy concepts and behaviours. A Likert Scale (1=not important at all; 7= extremely important) was used to gauge participants' perceptions and data reported in Table 5. Overall, participants indicated privacy as having importance,

evident in 28.3% and 40.0% signaling 5 and 6 respectively on the scale, while those who indicated privacy as extremely important numbered 26.7%. There were no participants who indicated privacy as having little, or no importance. This is an important finding, indicating participants perceived privacy as having importance and value.

Table 5.
Participants' Perceptions of Importance of Privacy

Degree Of Importance	Percentage of Perceptions							
	Not Important At All	1	2	3	4	5	6	Extremely Important
	1	2	3	4	5	6	7	
How Important is Privacy to You	0.0	0.0	1.7	3.3	28.3	40.0	26.7	

Note: N=60.

2.3.1 Comparison to Family/Friends' Privacy Needs

Data analysis also sought indications of participants' need of privacy in comparison to family and friends. A Likert Scale (1=less important; 7= more important) was used to determine comparisons and data are reported in Table 6. When compared with caregivers, 41.0% of participants saw themselves as having similar need of privacy, while 10.0% perceived their need of privacy as more important than their caregiver(s) needs. Interestingly, when comparing themselves to friends, 31.7% regarded themselves mostly similar to friends, 6.7% had greater privacy needs, while a much smaller percentage believed their needs to be less than friends' needs.

Table 6.
Participants' Perceptions in Comparisons of Privacy Needs

Percentage of Participants' Perceptions							
Need Of Privacy	Less Important						More Important
	1	2	3	4	5	6	7
Compared to Caregivers	0.0	3.3	11.7	45.0	23.3	6.7	10.0
Compared to Friends	1.7	3.3	8.3	31.7	21.7	26.7	6.7

Note: N=60

In summary, findings show privacy has importance to participants and their need of privacy was comparable to caregivers and friends. A small percentage saw their needs as distinctly less or more important. The next section looks at influences participants considered integral to their development of privacy concepts.

2.4 Influences in Development of Privacy

Understanding how participants' privacy concepts and behaviours may have developed in relation to influences they considered integral, were explored. Data in Table 7 reports qualitative comments related to these influences. Responses were largely lists of sources of influences with little elaboration on how exactly these had been executed, or their effectiveness. Interestingly, family members were prevalent influences, and included parents, siblings, grandparents, and wider family, and were represented in 40.0% of responses. Unsurprising, was the mention of classmates and/or friends who had been influential, and were 13.0% of responses. However, the slightly higher percentage of participants (16.0%) who indicated teachers and schools were influential was a positive indication. A

further 3.0% cited educational resources as having had some influence, for example “cyber-bullying video” (Survey Respondent # 43). Examples of responses from groups that indicated family, peers, teachers, and school resources as influential, are presented in Table 7.

Some participants noted that ‘experiences’ had an influence on their concepts of privacy, for example “travels” (Survey Respondent #55), and “gossip” (Survey Respondent #40), and featured in 8.0% of responses. Unspecified rules and agreements had also shaped some participants’ concepts and were indicated in 8.0% of responses. There were other influences noted by participants that demonstrated a multiplicity of sources, and while only a few mentioned these, they were nonetheless important to these groups. Specified sports clubs and coaches featured in 2.0% of responses. Similarly, church and Bible in Schools numbered 2.0%, while one participant specified Police, and Media/technology such as television and websites was cited by 3.0% of participants. A small number of participants stated they were unsure of influences that had shaped their privacy notions and practices. Findings are significant as they suggest confluences and outliers in participants’ ideas of whom and what has been important in privacy development. The role family took appeared crucial in the development of participants’ concepts and practices, and in addition, teachers and schools, and peers were noted as significant influences to some.

The table below reports qualitative data related to influences participants identified as contributors in the development of privacy concepts and behaviours.

Table 7.
Perceived Influences on Development of Participants' Privacy Concepts and Behaviours

Perceived Influences on Development of Privacy Concepts and Behaviours	Percentage of Comments
Close Associations	
Family	
<i>Citation Examples:</i> My parents have told me about privacy before (Survey Respondent #1); Mum and Dad...(Survey Respondent #18); My grandparents (Survey Respondent #24); my family explained on how to keep my details private online (Survey Respondent #29); My big brother and sister who have had social media before I started using it (Survey Respondent #38); My parents because they are very protective of things like their business...(Survey Respondent #4); My parents warning me...(Survey Respondent #11); Mum...(Survey Respondent #19); Cousins (Survey Respondent #22); My grandparents (Survey Respondent #24)	40.0
Peers	
<i>Citation Examples:</i> ...friends and their problems (Survey Respondent #40); ...my friends have influenced me (Survey Respondent #11); friends (Survey Respondent #33) Other classmates (Survey Respondent #52); ...my friends (Survey Respondent #9); ...friends have influenced me. (Survey Respondent #16); Friends (Survey Respondent #20); ...friends (Survey Respondent #27)	13.0
Educational	
Teachers	
<i>Citation Examples:</i> ...and teachers have influenced me (Survey Respondent #3) School have helped me a lot (Survey Respondent #13); Staff have influenced me about privacy (Survey Respondent #17); School teachers (Survey Respondent #39); My old primary school (Survey Respondent #5); Teachers (Survey Respondent #22); My teachers (Survey Respondent #36); School has influenced me a lot (Survey Respondent #51)	16.0
Educational Resource	
<i>Citation Example:</i> ...cyber bullying videos made me think about what is really out there in the internet world (Survey Respondent #43); Knowing what to do online from education (Survey Respondent #18)	3.0

Organisations	
Citation Examples:	
Sports Team (Survey Respondent #26); Coaches (Survey Respondent #53)	2.0
Church (Survey Respondent #49); Bible in Schools (Survey Respondent #25)	2.0
Police (Survey Respondent #39)	1.0
Experiences	8.0
<i>Citation Examples:</i> ...gossip (Survey Respondent #40); Travels (Survey Respondent #55); Experiences (Survey Respondent #41); Hearing about other people's experiences online (Survey Respondent #18); Experiences (Survey Respondent #50); There was hacking at our school and it taught me ... (Survey Respondent #59)	
Media - TV and Internet Sites	3.0
<i>Citation Example:</i> cyber safety advertisements... (Survey Respondent #48); Websites, most of them would ask to be careful online... (Survey Respondent #40); The T.V (Survey Respondent #58)	
Rules/Agreements	8.0
<i>Citation Examples:</i> I have seen some rules to keep all of your information private (Survey Respondent #21); Rules at school (Survey Respondent # 22) Rules from my parents (Survey Respondent #52); Rules (Survey Respondent # 49)	
Unsure	3.0
<i>Citation Examples:</i> I don't know (Survey Respondent #31); Not Sure (Survey Respondent #14); I'm not sure (Survey Respondent #11)	
Note: N=140 (Number of comments).	

In summary, this first section looked at broad ideas and examples of what privacy meant to participants. Their concepts and examples were reflected in contexts of the personal, social, and physical self, and findings suggested similarities in how participants valued privacy in relation to their perceptions of family and friends' value of privacy. Influences identified by those in this study showed family were integral in their development of privacy concepts and behaviours, and the role educational organisations and peers had performed in this development, also featured. Concepts and examples of privacy were frequently interlaced with online activities and device(s), as evident in citation examples shared in the tables. The next section investigates technologies used, online activity, and caregiver mediation/oversight in participants' online lives.

3. Digital Devices, SNSs, and Caregiver Mediation/Oversight

This section looks at participants' use of digital devices, their use of online SNSs/Apps, and caregiver mediation/oversight of devices and online activities. It presents descriptive data relating to these findings.

3.1 Digital Devices

Identifying participants' access and ownership of types of digital devices was important to this study to determine ubiquity of devices and any autonomy of use, as these factors may have implications on privacy concepts and behaviours. The digital device(s) participants' used and the ownership status appropriated to these, showed clear delineation between sharing and owning, as reported in data in Table 8. Only 7.0% of respondents indicated they shared an iPad, iPod or tablet device, and in contrast, a large number (87.0%) owned their device(s). Computers were shared by 22.0%, while only 7.0% owned one; Smartphones were not shared, and those indicating they owned one, numbered 63.0%; also, Wi-Fi or Bluetooth technologies were used by 48.0% of participants. Findings indicated participants had high levels of access to a device(s), and highlighted the large percentage that owned one or more Internet-ready mobile device(s). This is an important finding, suggesting the potential for many participants to achieve autonomous use of an Internet-ready mobile device.

Table 8.
Ownership and Type of Digital Device(s) Participants Use to Access the Internet

Participants' Digital Device(s) and Status of Ownership	Percentage of Responses
Own a Smartphone	63.0
Own a Tablet, iPad or iPod	87.0
Own a Computer	70.0
Share a Smartphone	0.0
Share a Tablet, iPad or iPod	7.0
Share a Computer	22.0
Use Other Wi-Fi or Bluetooth Technologies	48.0

Note: Total exceeds 100% as some participants indicated more than one device is shared or owned. N=60.

3.2 SNSs/Apps, Creation of Accounts, and Age Restrictions

Data relating to participants' preference and prevalence of use of SNSs/Apps, online account creation, and awareness of age restrictions, provided important information for this study. Findings indicated converging and diverging online practices that may in turn affect participants' privacy of information and content. Participants' use of particular SNSs/Apps that were listed in the survey was documented and summarized - data on this is reported in Table 9. It is important to note that almost all of the SNSs/Apps included in the survey questions were rated 13+ years. Equally important was participants' age at the time of this study, all being under 13 years. The most prevalent SNSs/Apps used were Snapchat, (85.0%); Instagram, (82.0%); YouTube, (78.0%); and Kik, with 62.0% of participants indicating use of this. Few participants used Ask.fm, or Tumblr, and those who used Twitter numbered 22.0%. Over half of the participants used Facetime, iMessenger, or Skype.

Further inquiry using a short response question into what particular SNSs/Apps participants preferred, sought to identify prevalence of use and preference, in contrast to general activity on SNSs/Apps. Data showed Instagram was the most favoured SNS/App, indicated by 41.0% of participants, and Snapchat was the next preferred App and numbered 26.0%. Facebook, Skype, and YouTube were preferred by smaller percentages of participants. Findings in Table 9 suggest that

while most participants indicated preference for particular SNSs/Apps, they were highly active across SNSs/Apps on device(s) that are largely mobile and owned by many of the participants. When these SNS accounts/profiles were made, and how aware participants were of any age restrictions, are considered in the next section.

Table 9.
Participants' Use of SNSs/Apps, and Comments Indicating Favourite SNSs/Apps

SNS/App	Percentage of Participants' Use	Percentage of Comments Favourite SNS/App
Facebook	28.0	10.0
Instagram	82.0	41.0
Facetime	68.0	3.0
Twitter	22.0	0.0
Snapchat	85.0	26.0
Skype	53.0	2.0
Kik	62.0	3.0
Tumblr	8.0	0.0
Ask.fm	5.0	0.0
YouTube	78.0	6.0
iMessenger	67.0	3.0
Pinterest		3.0
Tanki Online		2.0
We Heart It		2.0

Note: Total exceeds 100% as more than one SNS/App was selected by some participants: N=60; Comments relating to favourite SNS/App: N=60.

3.2.1 Creation of Account/Profiles and Awareness of Age Restrictions

How long participants had been associated with a SNS was of interest to this study to determine the nature of underage association(s) with any SNSs.

Underage use of SNSs/Apps suggests fictitious information has most likely been uploaded, and privacy settings may potentially be defaulted to those over 18 years, depending on the fictitious birthdate uploaded, and the SNSs used. Survey questions 14 and 15 inquired when approximately a preferred SNS account or

profile was made, and whether participants were aware of any associated age restrictions. Data relating to this are reported in Table 10.

Indications show only 5.0% of participants had created an account/profile in the current year (2015), while those who created profiles or accounts in 2014 numbered 46.0%, and those who had created one in 2013 were 32.0%. A very small percentage of participants had made an account as early as 2009 through to 2012. Only 2.0% could not recall when an account/profile was made. Findings show the majority of participants had created accounts in the last three years. Of concern is the duration many participants have been active on age restricted SNSs. As all participants in this study were under 13 years, this implies many were only 10, 11, or 12 years of age when their SNS accounts/profiles were created.

In addition to when account/profiles were made, information was sought on participants' awareness of any age restrictions accompanying their preferred SNSs. The intention was to ascertain how informed participants were of any accompanying restrictions. Data reported in Table 10 indicated 42.0% were unsure of any restrictions, and those who were fully aware an age restriction existed, were also 42.0%, while participants who believed no age restriction applied, numbered 16.0%. Findings show respondents were mostly aware or had no awareness at all of any age restrictions. This suggests age restrictions on SNSs held little interest or consequence to participants who were all active on SNSs in which they did not comply with age requirements. This raises concerns related to participants' underage activity on SNSs, their privacy, and exposure to potential online challenges and risks. Such concerns are discussed in detail in Chapter Five. In association with prevalence of underage use, the role of caregivers in mediating or overseeing participants' online activity and use of devices was of interest to this study, and is explored in the following section.

Table 10.
Participants' Profile and/or Account Creation, and Awareness of Age Restrictions on Favourite SNSs/Apps

Year of Account/Profile Creation	Percentage of Comments
2015	5.0
2014	46.0
2013	32.0
2012	5.0
2011	3.0
2010	3.0
2009	2.0
Year Unknown	2.0
Account or Profile Not Made By Participant	2.0

Awareness of Any Age Restrictions on SNSs/Apps	Percentage of Responses
Yes It Is Restricted	42.0
No It Is Not Restricted	16.0
I Am Not Sure	42.0

Note: Responses relating to creation of account/profile: N=60; Responses relating to any SNSs/Apps age restriction awareness: N=60.

3.3 Caregiver Mediation and/or Oversight

The nature or extent of any caregiver mediation/oversight was explored through a number of survey questions and data are reported in Table 11. The ability for caregivers to use participants' devices, and whether they had any linked online accounts/profiles was of particular interest. Those who indicated caregivers could use their device with no required password needed, were 8.0%, and in contrast, 45.0% signaled that access was enabled through a shared or known password. Of interest was the significant number of caregivers who could only gain access with participants' assistance, and this was indicated in 47.0% of responses. A large number of caregivers of this group could not gain access or use their child's device if they desired or needed to, that is, they were effectively 'locked out'.

In addition, caregiver connections to participants' SNSs and profiles/accounts were examined as an aspect of mediation/oversight. Those caregivers, who had access to more than one SNS account/profile were indicated in 50.0% of responses, while links with only one SNS numbered 28.0%, and those who had no links to any of the participants' SNSs, were 22.0%. Findings show a large percentage of caregivers had an association with one or more of participants' SNSs.

Table 11.
Caregiver Access to Participants' Device(s), and SNS/App Accounts or Profiles

Caregiver Access	Percentage of Responses
To Participants' Device(s)	
Access Without Password	8.0
Access With Shared Password	45.0
Cannot Access Without Participant Enabling	47.0
To Participants' SNSs/Apps Through Linked or Shared Profiles/Accounts	
Nil SNSs/Apps	22.0
One SNS/App	28.0
More Than One SNS/App	50.0

Note: Responses related to devices: N=60; Responses related to links: N=60.

Links between caregivers and participants' SNSs/Apps, through shared profiles or accounts were examined, to provide insight into this particular practice of connectivity or mediation. In addition, any correlations to participants' favoured sites could be identified. The data are reported in Table 12. Caregivers who had access to all of their child's SNSs/Apps was indicated in 6.0% of responses, while those who signaled their caregiver(s) had no links, were 9.0%. Instagram was the most linked profile/account with 20.0% indicating this. Facebook and Snapchat were indicated in 14.0% and 10.0% of responses respectively. Smaller percentages indicated iMessenger, Facetime, YouTube, Skype, and Kik were linked, while individual participants indicated Pinterest and Viber were linked.

In summary, some caregivers were able if desired, to access and/or participate in their child's SNS/App activities. The nature and utilisation of this connection is not clear, and if utilized, it may or may not be to interact and/or oversee activity. Instagram, Snapchat, and Facebook were the three most favoured SNSs/Apps and interestingly, these were the three most linked to caregivers.

Table 12.
Caregiver Access to SNS/App Accounts or Profiles Participants Use

Caregiver Access Through Linked Or Shared Accounts/Profiles	Percentage of Comments
Facebook	14.0
Instagram	20.0
Snapchat	10.0
Kik	4.0
Email	6.0
YouTube	4.0
iMessenger	9.0
Skype	6.0
FaceTime	5.0
Viber	2.0
Pinterest	3.0
Mobile Phone	2.0
All My SNSs/Apps	6.0
None of My SNSs/Apps	9.0

Note: N=96 (Number of comments).

3.4 Mediation and/or Oversight Strategies Employed by Caregivers

Data were gathered regarding any 'rules' or agreements caregivers had established in homes relating to the use of digital device(s) and/or online activities. The intention was to further understand any possible relationships or influence between mediation/oversight by caregivers, and the privacy concepts and behaviours of participants. Qualitative data were categorised and are reported in Table 13.

Those who signaled that no agreements or rules were expected of them at home numbered 6.0%, while a much larger number (40.0%) indicated caregivers expected their children to behave in responsible and respectful ways when online. Some comments specified what these behaviours entailed, however it was not clear how caregivers had conveyed, managed, or monitored these expectations or guidelines. Citation examples illustrative of this large group are presented in Table 13.

Adherence to age restrictions on some SNSs/Apps was noted as a rule/agreement in 6.0% of responses, while those who indicated certain SNSs/Apps had to be pre-approved before use, were only 3.0%. Some participants indicated caregivers controlled aspects of time online and two distinct facets of this emerged in the data. These were described as a duration of time allowed online, or specified times of use, with 12.0% and 11.0% indicating this respectively. The right to view participants' online activities featured in 4.0% of responses, while those who reported caregivers' rights to confiscate or delete device(s) or SNSs/Apps was only 3.0%. Requirements relating to the storage of a device(s) and when this is to occur, for example "...put all of my devices out of my room at night" (Survey Respondent #44), were indicated in only 5.0% of participants' responses. Citation examples characteristic of these groups are included in Table 13.

Findings showed a large number of caregivers had communicated behavioural expectations to participants related to device(s) and/or online activities. Also indicated in the findings was caregiver oversight or mediation using strategies such as viewing their child's online activity, limiting age restricted material, setting pre-requisites, time limits, or schedules, or removing devices if necessary. Participant compliance or non-compliance was not explored, nor did participants provide this information. Caregiver mediation/oversight is discussed in detail in Chapter Five. The next section presents data of participants' perceptions of how aware their caregivers were of their general online activities.

Table 13 reports qualitative data, relating to caregiver strategies used to mediate or oversee participants' use of devices and online activities.

Table 13.
Participants' Qualitative Comments Categorized, of Caregiver Mediation and Oversight Relating to Participants' Use of Digital Device(s) and Online Activity

Categories of Caregiver Oversight/Mediation Strategies	Percentage of Comments
Storage/ Location of Use of Device(s) <i>Citation Example:</i> ...put all of my devices out of my room at night (Survey Respondent #44); I have to give them my iPod and iPad at night time (Survey Respondent #53); ...not allowed it when I walk around town..(Survey Respondent #52)	5.0
Expectations of Appropriate Online Behaviours <i>Citation Examples:</i> No posting rude things (Survey Respondent #53); No bullying (Survey Respondent #55); Not allowed to give info out to strangers (Survey Respondent # 52); I am never allowed to let anyone on my account (Survey Respondent #46); Respect it (Survey Respondent #25); On Facebook if I say or do anything stupid I can't use it (Survey Respondent #6); Not to sign in with strange websites (Survey Respondent #11); If I do something bad on my device I will get it confiscated (Survey Respondent #18); I am not allowed to give out personal stuff and I'm not allowed to put up photos of me or any other people (Survey Respondent #25); Don't do inappropriate things...say unkind things...go on inappropriate sites...cyber-bully other kids (Survey Respondent #28); Use privacy settings (Survey Respondent #42)	40.0
Rules of Site/App Age Restrictions Applied <i>Citation Examples:</i> 13 if they are age restricted (Survey Respondent #56); R16 and over mum looks at it monthly (Survey Respondent #14); They allow me to watch some things but there are restrictions (Survey Respondent #55)	6.0
Right To Remove or Confiscate Device or Apps <i>Citation Example:</i> ... I'm not allowed to use my ipad or laptop or phone too much or they take it off me (Survey Respondent #48); ...and they can take it away whenever (Survey Respondent #5)	3.0
Right To - View Online Activity <i>Citation Example:</i> ...only allowed on Facebook when my dad's watching me most times (Survey Respondent #32); ...mum has to be allowed to look at all my accounts (Survey Respondent #8)	4.0
Specified and/or Restricted SNSs or Apps <i>Citation Example:</i> Not allowed a Facebook until 13 years old (Survey Respondent #38); What sites I'm allowed to sign up to (Survey Respondent #59)	3.0

Prerequisites of Tasks Prior to Use	3.0
<i>Citation Example:</i> Never before homework (Survey Respondent #10); I have to have done homework before using it each night (Survey Respondent #5)	
Permission Required Before Use of Device and/or Apps/Sites	7.0
<i>Citation Example:</i> That I have to ask to go on it at home...must ask before I game on it (Survey Respondent #55); I have to ask mum or dad to get any apps (Survey Respondent #9); No going on anyone's device without their permission (Survey Respondent #42); ...not allowed to create another social media account like FB unless they know first (Survey Respondent #48)	
Time:	12.0
Restrictions: <i>Citation Examples:</i> I'm only allowed one hour a day on week days (Survey Respondent #31); 20 mins to 40 mins (Survey Respondent #20); can only go on electronics for 30 mins on the week day and 45 mins on the weekend (Survey Respondent #4); Time limits ...(Survey Respondent #16)	
Scheduled:	11.0
<i>Citation Examples:</i> No Wifi in the morning (Survey Respondent #30); No devices after tea (Survey Respondent #4); No devices after tea... (Survey Respondent #6); ...after homework 10 mins (Survey Respondent #10)	
No Rules or Agreements	6.0
<i>Citation Examples:</i> No (Survey Respondent #3); No (Survey Respondent #20); idk (I don't know) (Survey Respondent #39)	
Note: N=107 (Number of comments).	

3.4.1 Caregiver Awareness of Participants' Online Activities

Participants were asked to indicate their perceptions of the degree of awareness caregivers had of their general online activities. I was interested in any relationships between participants' perceptions of caregiver awareness, and data on caregiver access and links. Data were elicited using a Likert Scale (1= not at all; 7= mostly all) and are reported in Table 14. The belief that caregiver(s) had very high awareness of mostly all their online activities was indicated by 17.0% of participants, while those who indicated reasonably high degrees of awareness, were 42.0%, and only 2.0% indicated no awareness at all. Findings showed participants believed their caregivers had moderate to high awareness of their online activities.

Table 14.
Participants' Perceptions of Caregiver Awareness Regarding Their Online Activities

	Percentage of Responses						
	No Awareness						Mostly Aware
	1	2	3	4	5	6	7
Degrees of Caregiver Awareness	2.0	5.0	6.0	8.0	20.0	42.0	17.0

Note: N=60.

In summary, access to, and ownership of digital devices and SNSs/Apps participants used, alongside caregiver mediation/oversight, was examined in Section Three. A large percentage of participants indicated they owned their mobile digital device(s), potentially enabling high degrees of autonomous mobile use. While all participants were under 13 years and users of at least one SNS, the majority was active across more than one SNS/App. While awareness of SNS/App age restrictions showed variance, it appeared that any age restrictions on sites were of little importance to participants in their use of SNSs/Apps. While participants' perceptions of their caregiver(s) awareness of their online activities appeared relatively high, possible inconsistencies were evident when paired with mediation/oversight strategies such as access to participants' device(s) and any links to SNSs. Suggested implications from key findings are further discussed in Chapter Five. Participants' perceptions, online actions, and influences are investigated in Section Four.

4. Perceptions, Online Actions, and Influences

The fourth section looks at participants' actions and experiences associated with their online activities and if there is any relationship(s) to their concepts of privacy. Of particular interest were the choices and actions undertaken, concerns expressed, and any ensuing actions in response to these concerns.

4.1 Actions Relating to P.I, Online Experiences, and Device(s)

How participants perceived and managed their P.I was of interest to this study in examining any relationships with their privacy concepts and behaviours, and data is reported in Table 15. In mitigating risks related to security and privacy, signing out of all online Sites/Apps once activities are finished is very important, thus concerns arise in relation to the percentage of participants (58.0%) who indicated they have forgotten to log out of SNSs/Apps. Also of concern, was the sharing of personal passwords, which is highly discouraged in many online site guidelines, Internet safety resources, and school policies. Those who indicated they had shared passwords numbered 43.0%, while those who had used others' passwords were 28.0%. Of surprise, was some participants' laissez faire approach towards allowing anyone to view their P.I, videos, and photos online, indicated in 15.0% of responses, and those who willingly shared P.I with unknown persons online, which were 3.0%. More indications that are positive were evident in those who indicated they had requested the removal of P.I, videos, or photos that had implicated the participant in some way, and numbered 53.0%. This suggests confident assertion, and knowledge and use of strategies required to initiate a request or actual removal of unwanted content. Concerns are raised across findings in the data that were elicited in this section. These issues are discussed further in Chapter Five.

Data were sought in relation to risky, empathetic, unethical online social contexts described in the survey questions, and any involvement participants may have had. One scenario outlined the action of defending or helping someone who was targeted online, and those who indicated they had, were 47.0%. Involvement in an online drama, argument, or fight featured in 32.0% of responses, however the degree or nature of participation was not examined. Pretending to be someone else online for unknown reasons was indicated in only 3.0% of responses, and those who had in some way hurt someone online, were only 2.0%. Of considerable concern were participants (12.0%) who indicated they had met up face-to-face with someone they had met online, and while the survey question sought no further information, this would be an important enquiry in the future. Those who had no experience of any online social contexts outlined, were 45.0%.

While these percentages indicating involvement are very small, the potential for challenges and risks to arise is possible, and of potential concern to the wellbeing of those participants.

Participants' actions related to their digital devices was explored, as an important aspect in evaluating privacy concepts and practices alongside particular actions. Contradictions were evident between privacy concepts of many participants, and practices that some undertook related to their device(s). Data reported in Table 15 reflected security and safety issues related to P.I and personal content stored on devices. Participants who allowed friend(s) to take away or use their device(s) featured in 58.0% of responses, while those who have used or taken away a friend's device(s) numbered 45.0%. Findings suggest relationships and trust are integral in these exchanges and more than half of participants indicated they had extended this level of trust to others.

Changing device settings, whether participants had allowed it or sought this from someone else, was also examined, and those who signaled they had no experience of these situations were 35.0%. Those who indicated they had changed settings on others' device(s) was 8.0%, while those who had their settings changed by someone else was 25.0%. These findings are important in illustrating motivational drivers, in that participants were willing to defer to others who had knowledge/skills to create changes on their device(s) that were desired, irrespective of any risks in doing so. Underlying motivations for these exchanges were not examined, and changes may have been problematic such as 'jail-breaking', or of no particular consequence. Potential challenges and risks relating to online and offline security, privacy, and safety, were evident in the findings, and these issues are considered in the next chapter.

The following table reports data pertaining to participants' actions and decisions in relation to P.I, devices, and social encounters described in the survey question.

Table 15.
Actions and Decisions Relating to Personal Information, Social Contexts Online, and Device(s)

Participants' Actions and Decisions	Percentage of Responses
Management of Personal Information	
Given Password Out	43.0
Used Someone Else's Password	28.0
Given P.I to Unknown Others Online	3.0
Don't Mind Anyone Viewing my P.I/Photos/Videos Online	15.0
Forget To Sign Out From Site/Apps/Email	58.0
Asked For Removal of P.I/Photo/Video Online	53.0
None of The Above	20.0
Social Actions Online	
Defended/Helped Someone Being Targeted	47.0
Pretended to be Someone Else	2.0
Been Involved in a Drama/Argument/Fight	32.0
Said or Done Hurtful Things to Someone	3.0
Met up Face to Face With Someone I Met Online	12.0
None of The Above	45.0
Actions Relating to Device(s)	
Let a Friend Take Away or Use My Device(s)	58.0
Used or Taken Away a Friend's Device(s)	45.0
Changed Settings on Someone's Device	8.0
Had Settings Changed on My Device by Someone	25.0
None of The Above	35.0

Note: Total exceeds 100% as some respondents indicated more than one action or decision under each section relating to Management of P.I, Social Actions Online, and Devices: N=60

4.2 Online Experiences

Unveiling types of concerns participants experienced online were important in examining how aspects might relate to their concepts and practices of privacy. A general impression of online encounters, and ensuing actions were elicited in survey question 25, and data are reported in Table 16. While many participants

had no experience of the specified scenarios, some others who had, indicated little concern. Of particular interest were those who signaled experience and concerns, and had either responded or chosen not to.

The most prevalent concerns indicated by participants were in relation to others' harmful or questionable behaviours online towards someone else. While the majority of participants indicated no experience of this, concerns were registered across the spectrum from somewhat concerned, through to highly concerned. Those who held significant concern were 20.0%, and those who were very concerned and did something were 20.0%. However, those who indicated they were very bothered but took no further action, numbered 8.3%. Observing or being a 'by-stander' to any online activity where a perpetrator targets a recipient raises concerns and implications from findings are discussed in Chapter Five.

When unknown people try to make contact online, this can invoke a sense of privacy invasion and/or concern, and this scenario was investigated in the study. Those participants who indicated they had not experienced this situation, were 40.0% of responses, while those who had experienced unwanted contact but were not concerned about this, numbered 35.0%. This encounter did generate concern for a smaller percentage (8.3%), and in response, they took further action. In contrast, those who indicated high concern in relation to an encounter but took no action were 5.0%. Participants were questioned further about unknown people, and the scenario of a stranger fabricating false information relating to participants was posed, and interestingly, a majority of participants indicated no experience, or little concern over this. A small percentage (5.0%) had encountered this scenario and though they were highly concerned, for reasons unknown they took no further action. Participants who did respond after experiencing high levels of concern in this situation, were 6.7%.

The scenario of fabricated information about a participant being shared online by others known to participants, was examined. Encouragingly, this situation was not experienced by many, nor did it raise serious concerns by most participants. However 2.0% did indicate high concern, but took no further action, while those who were very bothered by this and did something were 5.0%.

Uploading photo/video images in which participants were identifiable onto SNSs/Apps by others was a prevalent activity, but of no bother to over half of participants. This was a considerable concern to a small percentage of participants, and those who indicated this but did not pursue further action were 5.0%, while those who did something about it, numbered 6.7%.

Another scenario examined participants' exposure to online content they interpreted as disturbing or inappropriate. Findings show the majority had no experience or little concern, however those few who were very concerned but undertook no further action, was indicated in 3.3% of responses. In contrast, those who took action when encountering this content were 13.3%. Questions elicited wide-ranging data from participants, and covered a broad spectrum of concern. Findings of particular interest were those whom in relation to encounters online were concerned but not highly, those who undertook further action, and those who did nothing in response to their degree of concern.

Table 16.
Participants' Online Experiences, Degree of Concern, and Subsequent Action

	Percentage of Responses				
	Nil Experience Of This	Was not Really Concerned About It	Was Concerned	Really Concerned But Did Not Do Anything	Really Concerned and I did Something
Strangers Trying to Connect	40.0	35.0	11.7	5.0	8.3
People I Know Saying Untrue Things	68.3	11.7	13.3	2.0	5.0

People I Don't Know Saying Untrue Things	78.3	8.3	2.0	5.0	6.7
People Doing things Online to Others that Aren't Okay	40.0	11.7	20.0	8.3	20.0
Photos/Videos of Me on Others' Sites/Apps	26.7	56.7	5.0	5.0	6.7
Seeing content That Was Disturbing or Inappropriate	63.3	11.7	8.3	3.3	13.3

Note: N=60.

4.2.1 Concerns Encountered Online

Examining the source of concern and subsequent actions arising from participants' online experiences was included in the study, to further explore how their privacy concepts and behaviours may relate to their concerns and actions, because of certain online encounters. Qualitative data from those participants who commented (63.0%), were categorized under sources of concern, and subsequent actions undertaken. Citation examples illustrative of comments from those who shared concerns are reported in Table 17.

The issues of strangers making contact online, and strangers posting inappropriate comments, were of concern to 20.0% and 5.0% of those participants respectively, suggesting levels of insecurity and disconcert arising in response to these actions by unknown persons. Participants also indicated concerns relating to encounters with people known to them, and the most prevalent activity was the uploading of nasty, teasing, and/or untrue comments, as indicated in 35.0% of responses. This finding draws attention to the prevalence of negative online behaviours observed

by participants in this group. The visibility of participants in others' uploaded photos and videos was of concern to 25.0%, while swearing and hacking by known others were problematic to 5.0% of participants in this group. However, these small percentages do not negate serious implications resulting from the online actions and encounters described by participants in these groups.

The range of scenarios participants shared, suggest underlying concerns over losing control of options, breaches of trust and compromised safety of content, all of which were shown to be important in privacy concepts from findings in this study. The qualitative data reflected participants' candid concerns, and in turn make this data significant. The next section explores actions undertaken in response to some concerns expressed by participants in these groups.

The following table reports qualitative data of participants' concerns encountered in different contexts online.

Table 17.

Participants' Qualitative Comments of Sources of Online Concerns, Categorized

Source of Online Concerns	Percentage of Comments
Strangers	
Making Contact:	
<i>Citation Examples:</i> People I don't know trying to connect to me (Survey Respondent #40); Someone I didn't know kept trying to follow me (Survey Respondent #24); Random people trying to follow me on Instagram...(Survey Respondent #4)	20.0
Strangers Posting Inappropriate Comments:	5
<i>Citation Examples:</i> A strange man said inappropriate things to me on Facebook...(Survey Respondent #29)	
Strangers Using Inappropriate Language:	5

 Known People

Known People Posting Nasty/Teasing/Untrue Comments: 35.0

Citation Examples: Sometimes I see people teasing others online...(Survey Respondent #48); A friend talking about me to a person that wasn't true (Survey Respondent #50); Bullying/calling mean names (Survey Respondent #37); Someone saying rude things about someone's voice...(Survey Responent #16); People were sending not very nice things...(Survey Respondent #42); Someone was cyber-bullying someone else and I told my mum and she rang ...(Survey respondent #44)

Known People Uploading Photos/Videos With Me In Them: 25.0

Citation Examples: An inappropriate photo of me (Survey Respondent #20); One of the students at school posted a picture saying how I used ... and said rude things about me (Survey Respondent #28); People posted group pictures with me in them on...(Survey Respondent #31); People posting photos of me on Instagram that I don't want on there...(Survey Respondent #50); There was a video that was of me put on youtube and I was okay at first but then a lot of people started to look at the video and it was okay for friends to see but everybody else saw it so I got really uncomfortable and told the people that put it up I wanted them to take it down but they still left is up there and it is still up there now (Survey Respondent # 54)

Known People Swearing: 5.0

Citation Example: People I know swear on websites (Survey Respondent #53); Swear words ...(Survey Respondent #60)

Known People Hacking: 5.0

Citation Examples: I was hacked on my Snapchat account...(Survey Respondent #58); A person hacking someone's Snapchat (Survey Respondent #59)

Note: N=46 Comments relating to source of online concerns.

4.2.2 Actions Undertaken in Response to Online Concern

Further comments were sought from those participants who shared concerns related to specific online scenarios. The actions some participants undertook in response to their concerns were shared, and qualitative data were categorized and

are reported in Table 18. It was apparent that the most common action was to tell someone, however the means by which this was conveyed was not well defined. In the first instance, most ‘spoke up’ directly to the perpetrator, as indicated in 21.0% of responses. One participant told a teacher, while those who told a caregiver numbered 17.0%. One participant shared they had not told anyone of their situation, and another participant described how they had supported a friend who was upset by an online concern, by talking through the situation with them. Of considerable concern was one participant’s response who indicated that as a result of an online encounter, they had engaged in self-harm, and in addition, went on to seek out this person and eventually reported the perpetrator, as illustrated in the citation “I had cut myself once due to social media and a ...was bothering me and I ended up finding the culprit and reporting ...” (Survey Respondent #46). This situation is further discussed in Chapter Five.

Employing tools available on device(s) and some SNSs/Apps was another strategy some participants indicated they had used to respond to online situations. Those who reported someone’s actions to a SNS/App featured in 12.0% of responses, while the most prevalent action was to block someone, and this was indicated in 30.0% of responses. Only one participant signaled they cleared their search history as a strategy. The table below reports the categorized qualitative data related to participants’ actions.

Table 18.
Participants’ Qualitative Comments Categorized, Relating to Actions

Categories of Actions Undertaken by Participants	Percentage of Comments
Speaking Out	
Spoke up to Perpetrator: <i>Citation Examples:</i> When people were sending not very nice things I told them "well do want people to be sending that to you? (Survey Respondent #42); Someone was being mean to someone else and I stuck up for the person (Survey Respondent #51); Told them it was cyber-bullying (Survey Respondent #29); Sometimes I see people teasing others online and I tell them to stop it (Survey Respondent #48)	21.0

Told a Teacher:	4.0
<i>Citation Example:</i> told a teacher...(Survey Respondent #43)	
Told a Caregiver:	17.0
<i>Citation Examples:</i> Someone was cyber-bullying someone... so I got my mum to ring that persons mum (Survey Respondent #44); I told my mum straight away (Survey Respondent # 29); told mum and dad about it (Survey Respondent #8); ...my parents ended up helping me through (Survey Respondent #45)	
Talked to Victim:	4.0
<i>Citation Example:</i> (Participant's friend encountered mean comments and was upset)... What I did was: I was being nice and told her (friend) that wasn't true and she should just delete those people contact, and not to have anything to do them (Survey Respondent #47)	
Have Not Told:	4.0
<i>Citation Example:</i> I was once bulled online when I first started and I never told anyone then it kept coming up again but, I still have not told anyone (Survey Respondent #45)	
Self-Harm	
Hurt One's Self:	4.0
<i>Citation Example:</i> ...I had cut myself once due to social media and a guy that was bothering me (Survey Respondent #45)	
Use of Tools and Settings	
Cleared my History:	4.0
<i>Citation Example:</i> I exited out of it cleared my history (Survey Respondent #8)	
Block People:	30.0
<i>Citation Examples:</i> Blocked them (Survey Respondent #10); I blocked them (Survey Respondent #9); I deleted his friend request (Survey Respondent #13); I blocked them and stopped following them (Survey Respondent #9); I just blocked them (Survey Respondent #5); Someone posted naked pictures of girls to see and then I blocked the person (Survey Respondent #46); ...and blocked them (Survey Respondent #29); I just don't let them follow me (Survey Respondent #48)	

Reporting to Site:

Citation Examples: ...social media... finding the culprit and reporting him 12.0
 (Survey Respondent #45); Reported it to the site (Survey Respondent #52); I just
 clicked on the report abuse button...(Survey Respondent #55)

Note: Participants' comments describing actions undertaken: N=24.

In summary, this fourth section reported a wide array of actions and decisions undertaken by participants, and scope of understandings, degree of concern, and subsequent actions. Considerable concerns and potential issues related to privacy, safety, and security across online and offline contexts surfaced in the findings. These are discussed further in Chapter Five. The next section investigated online tools and settings participants used, and their perceptions related to competency in managing their online privacy, safety, and security.

5. Knowledge and Use of Online Tools and Settings, and Perceived Competencies

An array of tools and settings are available on many devices and SNSs/Apps enabling user options to personalize, customise, and restrict access and visibility of their information and content. This section reports data showing participants' use of online tools and settings and perceptions of capability in managing their online privacy.

5.1 Online Tools and Settings

A range of online tools designed to protect and secure content were investigated, and data are reported in Table 19. These data were included as it provided insights into how aware or active participants were in employing specific measures available on devices that can aid and protect online content and P.I. Locking down a device so a screen is secure from unwanted access can be achieved through various tools. These include the use of passwords or code protected access, with 93.0 % of participants indicating use of these. Those who

have an iPod, iPad, or iPhone, may employ an App used to find their device(s) and 42.0% indicated they have this installed. Using a timer to close down one's screen as a security measure is utilized by over a half of participants, and Power-Down or Sleep-Mode is used by over half of participants. While a finger scanner is a relatively new tool built into some devices, those who indicated use of this were 15.0%. Also indicated in nearly half of participants' responses were the practices of logging out of sites and regularly clearing History and/or Cookies. Participants indicating use of strong passwords was 78.0%, while those using different passwords for various sites and Apps and was 40.0%.

Findings indicated participants employed some tools and settings, providing a measure of security and privacy of P.I. Contradictions in privacy concepts and practices were found between the majority who indicated employment of strong passwords, and earlier findings whereby many participants shared theirs or used others' passwords.

Table 19.

Participants' Use of Privacy and Security Tools on Device(s)

Tools and Settings Used On Devices By Participants	Percentage of Responses
A Password or Code Protection	93.0
'Find my iPad' or iPhone App Installed	42.0
Timer Which Locks Screen	55.0
Finger Scanner	15.0
Power Down or Sleep Mode	58.0
Firewall, Anti-virus, Anti Malware and Similar Software	32.0
Logging Out of Sites Requiring Personal Passwords	48.0
Clearing History and/or Cookies Regularly	47.0
Use Passwords at Least Eight Characters Long	78.0
Different Passwords for Different Sites/Apps	40.0

Note: Total exceeds 100% as some participants selected more than one tool: N=60.

5.2 Status of Profiles and Awareness of ‘Public’

The use of the word ‘public’ in this study was associated with SNSs/Apps and implied openness to the online global community, and whether this community had access to participants’ content from anywhere, at anytime. Data reported in Table 20 reflected participants’ levels of awareness of how public their profiles were to this global community. Responses indicating participants used recognisable photos of self on their public profile(s) numbered 50.0%, and actual birthdates visible to the public featured in 15.0% of responses, while visibility of one’s school, home address, or sports club, numbered 32.2%. Encouragingly, a significant number of participants do not have a phone number visible on their public profiles, as indicated in 93.0% of responses. A large percentage of participants were active in deleting contacts or ‘friends’ as indicated in 93.3% of responses, and those aware of how many contacts or ‘friends’ can view their content, numbered 83.3%. These indications suggest many participants were relatively aware of those they have given rights to fully access their personal content on SNSs/Apps. Similarly, the larger number of participants who indicated they have deleted ‘friends’, suggests conscious decisions were made at times to discontinue access of selected ‘friends’.

Table 20.
Participants’ Personal Information in Public Profiles on SNSs/Apps

	Percentage of Responses		
	Yes	Not Sure	No
Awareness of Personal Information in Profiles on SNSs/Apps			
Recognisable Photo of Self in Public Profile	50.0	20.0	30.0
Birthdate Visible in Public Profile	15.0	8.3	76.7
Phone Number Visible in Public Profile	3.3	3.3	93.3
School, Home Address, Sport or Club Visible in Public Profile	23.3	13.3	63.3
Know Number of ‘Friends’ and Contacts	83.3	8.3	8.3
Deleted ‘Friends’, ‘Followers’ and Contacts	93.3	3.3	3.3

Note: N= 60.

Findings signified uncertainty in some participants' level of awareness of how public their profiles were. Issues were evident in who exactly had access to important P.I of participants involved in this study. Gaps were evident in participants' awareness of what constitutes 'public' and the risks and challenges associated with this. In addition, participants' willingness to share their P.I publicly was of concern, if they were fully cognisant of what 'public' denotes. Some did indicate considerations in keeping certain P.I private, however, participants' knowledge of others' rights and opportunities to copy, publish, steal, re-post, or change information, are not well known, and inherent risks are possible. Implications relating to visibility to the online public are discussed in the proceeding chapter.

5.3 Attitude and Capability in Using Specific Online Tools and Settings

How capable, active or interested participants were in using particular tools, settings or site information, was investigated and data are reported in Table 21. It was important to ascertain participants' attitudes and capability so that associations or disconnects with their concepts and practices of privacy might be identified. Attitudes of ambivalence, perceived lack of need, or lack of knowledge in using stated tools were indicated in small percentages, but nonetheless, raise awareness of needs and concerns.

Those not interested in reporting anything disconcerting or wrong to a site/app, were 25.0% of responses, while those who would if they knew how, featured in 28.3%. Utilisation of privacy settings to control visibility of content was indicated by 80.0% of participants, however those not interested in knowing how to, numbered only 5.0%. In contrast, those who would like to control privacy settings but lacked knowledge to do so, were 8.3% of responses. Over half of participants considered themselves capable in finding out about site terms and privacy statements, however those who indicated capability but chose not to, were 13.3%, and a further 13.3% of participants were not interested in knowing.

The wide-ranging responses were an important finding. Of concern were those who indicated they lacked the knowledge to perform certain actions, as well as those who were not interested in knowing, indicating that a gap of understanding existed in participants' knowledge of how to perform online tasks was evident. This has implications for participants' understandings of the necessity or desirability in managing potential challenges or risks, and protecting one's privacy and security. These are discussed further in the next chapter.

The following table reports the data related to participants' knowledge and use of online tools.

Table 21.
Participants' Knowledge and Use of Online Privacy and Security Tools

Knowledge and Use Of Online Privacy And Security Tools	Percentage of Responses			
	Yes, When Necessary	I would, But Don't Know How	No, Not Interested in Knowing	No, I Know How but Don't Bother
Clear Recent Searches/Cookies	65.0	13.3	10.0	11.7
Edit/ Delete My Online Content	83.3	5.0	3.3	8.3
Find Out Terms and Privacy Policies of how my Information is Stored and Used	60.0	13.3	13.3	13.3
Use Privacy Settings to Select Who Sees my Posts/Information	80.0	8.3	5.0	6.7
Report to the Site When I see Anything Wrong or Concerning	38.3	28.3	25.0	8.3
Delete or Deactivate Account or Profile	61.7	5.0	16.7	16.7

Note: N=60.

5.4 Perceptions of Capability in Management of Online Privacy

To determine participants' perceptions of their overall skill, knowledge, and capability in managing their online privacy and safety, a measure was used. A Likert scale (1= not confident, skilled or knowledgeable; 7= highly confident, skilled and knowledgeable) elicited data that are reported in Table 22.

Participants who perceived their capability to be high, were 20.0%, while many others saw themselves as having some levels of confidence and capability, and numbered 22.0%, and 40.0% respectively. Only a small percentage (3.0%) signaled slightly less capability and confidence, and no participants perceived themselves as unskilled or lacking confidence. In general, data showed participants believed they were highly competent in managing their online privacy and safety considerations.

Table 22.
Participants' Perceptions of Capability in Managing Their Online Privacy and Safety

	Percentage of Participants' Perceptions						
	Not Confident, Skilled or Knowledgeable						Highly Confident, Skilled and Knowledgeable
Participants' Perceptions	1	2	3	4	5	6	7
	0.0	0.0	3.0	15.0	22.0	40.0	20.0

Note: N=60.

6. Summary

This chapter presented data related to participants' privacy concepts and privacy practices in both offline and online contexts. Strong values, concepts, and behaviours emerged in early findings related to privacy in participants' lives. However, actions and decisions made in some online contexts were not always aligned to participants' privacy concepts. Attitudes and capabilities in online

contexts were not always consistent with the values and practices of privacy of some participants. Most participants regarded themselves as proficient in managing their privacy across contexts, however exposure to potential challenges and risks were noted across findings. The proceeding chapter discusses key findings in relation to research.

Chapter Five: Discussion

Introduction

The research question explored preteens' broad concepts of privacy, and how these may have developed; and in conjunction, examined any relationship(s) with their actions and decisions on Internet-connected devices and online social environments. This chapter considers the emerging aspects suggested by the findings in relation to the research questions. These aspects are discussed under headings and sub-headings across six sections.

The first section focuses on participants' perceptions of what privacy is and examples of privacy importance in their lives. The second section considers aspects of participants' privacy concepts relating to self that emerged from the findings. These were categorized under three dimensions of the personal, social, and physical self, and aspects relating to these are explored. The third section looks into the development of privacy and examines influences involved in the formation of participants' privacy concepts and practices. Digital device use, underage use of SNSs/Apps, and inconsistencies in participants' online activities that emerged in the data, are discussed in the fourth section. In the fifth section, caregiver mediation and oversight strategies relating to participants' devices and online activities are the focus of discussion. The sixth section explores participants' perceptions and actions associated with online challenges, and in addition, examines issues linked to the visibility of participants' personal information in online environments. A brief summary concludes this chapter.

1. What is Privacy?

Participants' extensive and wide-ranging descriptions relating to their perceptions of privacy were an encouraging and unexpected finding. Of interest are participants' concepts of privacy and the interconnection with examples of privacy importance in both their *offline* and *online* lives. The first section of the study sought to elicit a broad lens on privacy, and made no overt reference to

online contexts, and therefore the volume of responses and inclusion of online and offline contexts by those who responded, signals an important finding. This indicates confluence between what many participants thought privacy was, and their conveyance of privacy importance in their daily lives, lived both online and offline. From these data, three key dimensions emerged in the findings relating to privacy, and were categorized as the *personal*, *social*, and *physical* self.

Underlying these dimensions were further aspects of privacy described as autonomy and control; personal information; personal belongings, space and solitude; relationships with others and exchanges of trust; physical safety, security, and one's body.

These dimensions and aspects of privacy are important findings and suggest three key factors. The first factor suggests participants' privacy definitions were not limited; on the contrary, they incorporated wide-ranging interpretations and expressions, and suggest a depth of maturity and insight that was somewhat unexpected. Secondly, confluence between participants' concepts of privacy and examples of privacy importance indicated their privacy concepts were robust and deployed in varied contexts. Thirdly, privacy concepts and behaviours appeared to be seamless across online and offline contexts.

Participants appeared to exercise various levels of control over their privacy through tacit or overt boundaries. This aligns with the theory that privacy is the process of regulating levels of social interaction with others, including control of access others have to aspects of one's self (Altman, 1977). Examples were evident in the way several participants expected to be consulted before someone used or took their possessions, for example not liking it when 'people feel they can go through my stuff without asking', and displeasure with people 'going into my room without my permission'. Control of access and use of boundaries were also seen in participants' responses relating to disclosure of information for example, 'not being able to take a photo of you without you agreeing to it'. Privacy has also been described as having different types and functions and is expressed through states of solitude, intimacy, anonymity, and reserve (Westin, 1967).

Aspects of this theory are evident in the qualitative data collected of participants' privacy concepts and privacy importance, and an emphasis on the one's rights and freedoms pertaining to their privacy was apparent. This was seen in the following examples. One participant shared that privacy was a freedom from being watched or stalked, some (19.0%) described their right to having their own space or belongings, and most indicated a right of freedom to choose who they share intimate information with, and their right to make decisions in regard to what they share.

1.1 Importance of Privacy

Participants appeared to have considerable regard for the importance of privacy in aspects pertaining to their relationships, possessions, personal affairs, information, personal space, and time alone. These aspects again traversed both offline and online contexts. Importance of privacy was indicated in the abundant examples that included contexts of home and school, when out and about, and when online. These were seen in responses that indicated privacy was important when online; in one's room; not being watched by people or stalked online and offline; and one's Internet life. Participants appeared to understand and value different facets of privacy across these contexts, aligning with Westin's theory that privacy is characterized through various types and functions (Westin, 1967). Participants' perceptions of any access others may have to their possessions, personal affairs, and personal space, suggest that participants felt strongly about having choice and control in the decision to on-share anything of personal value with select others. This negotiation of control further supports Altman's theory, that privacy is based on socially negotiated contexts, as well as cultural influences (Altman, 1977).

Just over half of all participants, in describing privacy importance, included types of P.I, and boundaries in relation to disclosure and/or secrecy of this. This was evident in the use of the pronoun 'my', and seen in responses that referred to privacy importance related to '*my* messages', and '*my* photos', and 'the stuff on *my* device'. Boundary control was seen in comments that referred to select people having access, for example 'secret, for your eyes only'; 'not showing your private

information/photos with the public’; and ‘your identity is not able to be seen by others that you do not want them to see’. An importance of privacy relating to certain P.I such as one’s name, age, address was noted in responses, along with examples that included a desire or right to privacy of one’s personal messages on phones, SNSs, journals and schoolwork. These findings indicate that privacy of P.I was highly valued by half of all participants, and the nature of relationships with others determined the degree of privacy need. Many had clear notions of what comprised P.I, and in turn, suggests they employed measures of regulating others’ access and disclosure of their P.I. This is evident in some comments that indicated they ‘kept things to themselves’, while one participant shared ‘I’m not worried about my privacy around people I know’, and another ensured ‘no randoms’ could see their personal information or images.

2. Privacy Aspects Across the Personal, Social, and Physical Self

The *personal, social, and physical self*, are three dimensions of privacy that emerged in the findings from the analysis of data related to participants’ privacy concepts and examples of privacy importance. These dimensions reflect the depth and scope of participants’ privacy notions, and are discussed individually in this section.

2.1 The Personal Dimension

Four aspects underpinned dimensions of the personal self, and respondents indicated these in both their notions of what privacy is, and in their examples of privacy importance. Aspects of autonomy and control, was evident in 59.0% of responses, and examples of P.I and issues of confidentiality was noted in 95.0% of comments. Participants made reference to privacy relating to personal belongings and featured in 8.0% of responses, while the desire for personal space and solitude was reported in 19.0% of comments. Autonomy and control, as aspects of privacy, are also integral elements of moral, cognitive, spiritual and emotional development (Schoeman, 2008). Examples of autonomy and control

are seen in responses that referred to one's control over access, such as 'not letting anyone see things because it is rightfully yours', and 'privacy is when you are able to do your personal things'. The ability to build trust, love, and friendships and to moderate these relationships, is built on one's ability to control aspects of self such as one's thoughts and one's body (Smetana, 2010). This autonomous thought and action is evident in the response one participant shared relating to privacy importance, 'you want to keep things to yourself', and another participant shared 'your ideas and your thoughts are left to yourself'. Findings indicate many participants were aware of, and purportedly executed degrees of autonomy and control over their affairs including their relationships, belongings, personal space, and personal information.

A predominant aspect of over half of all participants' privacy notions pertained to types of personal information. Comments indicated a desire to retain confidentiality, and/or control of disclosure of their P.I in either online or offline contexts. Also, due to the affordances of digital technologies participants shared their P.I through a variety of modalities. These modalities are designed to engage one's senses, and examples are seen in participants' references to information being shared via these modalities. This was seen in responses that indicated need for privacy in relation to emails, texts, written notes, and mail, phone calls, face-to-face conversations, Skype, and online content comprising images such as photos and videos. Internet-connected technologies have evolved rapidly and enable new conduits and highly engaging forums for sharing one's P.I. These in turn require new considerations of control and boundaries, as well as rights and regulations in relation to one's privacy. This is crucial for young people as they endeavour to navigate online environments which are largely unregulated and unsupervised (Livingstone, 2008).

Parker's concept of privacy is seen as the controlling of any access others may have to aspects of ourselves that can be sensed (Parker, 1974). This is an interesting point for discussion in relation to the affordances of new technologies that engage young people's senses, and the diverse challenges involved in managing one's privacy. This may be particularly so when a prevalence of access

and use of digital technologies is afforded to many young people. This prevalence was evident in the data that indicated most participants owned a tablet, iPad, or iPod, as well as a smartphone, and in addition, a laptop or computer.

These engaging modalities may essentially distract young people in understanding issues related to visibility of their P.I online, and others' access to this. These modalities may also encourage disclosure of P.I to various known, and unknown audiences through the design interface of some sites. Many sites encourage users to disclose a range of P.I solely because spaces and boxes exist that require or invite users to submit information (De Souza & Dick, 2009). The design interface is often confusing and difficult for users to navigate, particularly for younger users (Christofides et al., 2012). Therefore, having greater technical knowledge and capability may enable younger users to navigate various social complexities in online environments, with greater degrees of confidence and understanding (Yan, 2009).

These factors may have contributed to inconsistencies evident in some participants' privacy behaviours and concepts of privacy, in relation to online contexts. For example, 15.0% of participants were unconcerned about the degree of visibility of their P.I online that included private information, photos or videos, and half of all participants were comfortable using a recognisable photo of themselves as their public profile picture. Almost half were unaware of whether the wider public had visual access to certain personal content such as their profile photos, birthdate, and address, and over half had experienced discomfort over others uploading their image or content online. The act of signing out of log-in sites is crucial to security of one's content, and over half indicated they were erratic in signing out of online sites. These examples could indicate that some may benefit from gaining further understandings of the social complexities within online sites regarding what they share, how and with whom it is shared, and possible implications involved in sharing. A deeper knowledge regarding the mechanisms, tools, and strategies available through the technologies and Internet

sites is also needed. This in turn may enable greater control over others' access, and disclosure of one's P.I both online and offline, in order to regulate levels of privacy young people require, desire, or need to consider.

Another aspect relating to P.I was the reference to 'secrecy' that was made. The notion that secrecy is both the concealment of P.I, and also avoidance of disclosure, lies at the centre of what is regarded as the constitutional right of privacy relating to one's P.I (Solove, 2002). Findings suggest secrecy was not exclusively about concealment and avoidance of disclosure, rather they signified disclosure was a measured process and involved selection of others. This was seen in responses, for example 'things I tell my best friend', and 'only me and the person are allowed to look', indicating there were some secrets that only a select few knew. This secrecy was at times extended to include another(s), such as a friend, caregiver, or teacher, and were accordingly privy to private and potentially sensitive information. By implication, 'group' secrecy was entered into, requiring degrees of trust and intimacy between parties, whereby this level of disclosure was perceived to be secure. The intricacies of concealment and disclosure with various others indicated in responses, supports the theory that privacy is a socially negotiated activity (Altman, 1977).

Aspects of solitude and/or a personal place were also seen in the findings of concepts and importance of privacy, and 19.0% of comments indicated this as the participant's bedroom, where they could be alone. This finding was not unexpected, and other studies concur that solitude is the space and place in which one can retreat from the scrutiny and interference of others (Hodkinson & Lincoln, 2008; Livingstone, 2002; Margulis, 2003). This was seen in the responses that included places such as one's bedroom; conceptual space such as one's 'personal bubble'; and 'having your own room that no one can go into...your own thoughts'. Several participants expressed a need to be alone to think and reflect, and a few sought some time alone without the distraction of others. These ideas align with Borbar's description that solitude provides an opportunity to decompress (Younger, 2015), and also enables opportunities for quiet contemplation and consideration of one's own world (Blatterer et al., 2010).

That so few participants reported these particular aspects, may perhaps be explained by the growing trend of filling the ‘gaps’ in one’s life with screen-time on digital devices in private and public spaces. These ‘gaps’ are the unscheduled times in one’s day, and could potentially provide opportunities when one could choose to be alone, to have time to self-reflect and decompress. Teens use SNSs and other sites as their ‘go to’ activity when they are bored and in need of a “time filling activity” (Awan & Gauntlett, 2013, p.120). This raises questions as to whether younger people are exchanging times of solitude and alone time, with online activity. If this is so, further questions surface as to any impact there might be on the wellbeing and development of younger people as they fill the ‘gaps’ in their lives with screen-time on digital devices. Further research is needed to understand if time to decompress and be alone with one’s own thoughts is being exchanged for connectedness online, and if so, what impact this may or may not have.

A small number of participants (8.0%), identified personal belongings as an aspect of privacy, and were evident in responses referring to ‘my device’, or ‘my stuff’. Interestingly, boundaries were suggested and attempt to regulate others’ access and in some instances, concealment. For example, having control over one’s ‘stuff’; others not helping themselves; not looking through their ‘stuff’; and keeping one’s site safe from unwanted scrutiny. Subsequently, an assumption is implied that others ought to observe these overt or tacit regulations and boundaries or by implication they would be invading or intruding upon those participants’ privacy rights. This relationship between others’ regard for one’s privacy boundaries and rules, and notions of intrusion or invasion if disregarded, are well-supported in other studies (Hawk et al., 2009; Parke & Sawin, 1979; Smetana, 2010).

2.2 Dimensions of Privacy: The Social Dimension

Relationships and the exchange of trust were important elements and notions of privacy for some participants (14.0%). The data points to disclosure of P.I as an exchange of trust that was negotiated with primarily family and/or friends, and affirms earlier findings that suggested ‘group secrecy’ is entered into with ensuing expectations of confidentiality and trust between these parties. Several participants alluded to a sense of invasion of one’s privacy if a trusted person on-shares their P.I, in the same way other participants felt a sense of privacy invasion when personal belongings were accessed without one’s consent.

However, inconsistencies were noted in later findings whereby a number of participants indicated they disclosed certain P.I with known and unknown others in online environments, for example one’s school, birthdate, club, and passwords. While findings suggest many participants had some cognisance of the notion of what is ‘public’, other findings indicate concepts of the public domain relating to online environments were not well understood by many participants. This was evident in the number of participants who were not sure about the visibility of some of their content on their SNSs, or were unaware if their P.I was in the public domain. Others lacked surety or skill in being able to adjust settings to manage visibility of content within an online site. For example, 70.0% of participants had either a recognisable photo of them on a SNSs public profile, or were not sure if they did; similarly, 23.0% indicated their birthdate was visible on their public profile, or were unsure if it was visible. This raises questions as to whether these participants were fully informed of the challenges and risks associated with sharing crucial P.I in the public domain online.

Making choices about one’s P.I from an informed position of what ‘public domain’ means, and others’ rights over this content, align with aspects of autonomy and control, and findings indicate inconsistencies between these. This is also evident in those who were unsure, implying unfamiliarity with the visibility of their own P.I, and tools and settings on particular SNSs/Apps.

Privacy is not only a social concept, it is also a behavioural concept (Margulis, 2003) and while aspects of privacy are socially negotiated between people, privacy behaviours or actions are necessary to open or close personal privacy boundaries. For example, responses indicate participants ‘told’ something to someone, or ‘showed’ private content to someone when trust was present in the relationship. However, if the person was unknown or untrusted, various actions ensued. This was seen in responses from several participants who had encountered concerns related to unwanted online contact and spoke or ‘messed’ the perpetrator directly to close access. Also, almost a third of those who commented on what action they undertook, indicated they had ‘blocked’ unwanted contact online.

While these examples suggest a conscious decision is made relating to access and disclosure, and implies control over the process of opening boundaries, it is important to note that some scenarios do not necessarily infer consent, as coercion could be a factor. For example, the act of ‘sexting’ (sending naked videos or photos of oneself to another) and the associated trauma for those coerced into this activity does not support the idea of control or choice, although a conscious action or behaviour has been undertaken to disclose very intimate content (Drouin, Ross, & Tobin, 2015). Findings indicate that many participants considered control and regulation of boundaries as a right, and executed degrees of choice in processes of disclosure, supporting the idea that privacy is both a social and behavioural concept.

2.3 Dimensions of Privacy: The Physical Dimension

Other studies suggest that having control over intimacies relating to one’s body is integral in privacy concepts (Inness, 1992; Kasper, 2005). Privacy was expressed by only a few participants (4.0%) as important in personal matters such as ‘going to the bathroom’, and was not an unexpected finding. Aspects related to one’s body and rights to manage intimacies related to this, are not uncommon to this age

group. However, given the physiological changes taking place at the onset of puberty, I assumed more participants might have identified this as a facet of privacy.

Of particular interest were the small number who indicated that privacy also included freedom from surveillance, and several noted that having physical safety and security from home invasions was of importance. Being ‘observed’ was another aspect noted by several participants who remarked that when, or if someone watches you, it is akin to ‘stalking’, and is essentially privacy invasion. While only a small number of participants conveyed these particular aspects related to one’s need for safety and security, they have highlighted the constitutional right to be safe and secure from acts of interference or harm by others (Blatterer et al., 2010).

3. Development of Privacy Concepts

This section considers developmental aspects that may have contributed to participants’ concepts of privacy, and some of the influences participants identified as important in the development of their privacy concepts. Privacy was both convoluted and multifaceted in the responses provided, and highlights that privacy development is not a ‘stand-alone’ aspect. Privacy descriptions provided by participants, suggest complex and diverse developments across many aspects of the self. These include the cognitive, social, cultural, moral, emotional, and physical characteristics associated with this preteen age (Harter, 2012; Moshman, 2011; Smetana, 2010). These developmental facets were evident in responses from almost all participants who indicated either a strong need for privacy; a need for security related to one’s body; desire for greater autonomy and control over their affairs; a sense and assertion of their rights over possession and P.I; and expectations of privacy placed on trust-based relationships.

These well-formed privacy concepts may have been constructed through cumulative experiences, developmental influences, and critical information gleaned over time and across contexts. This is referred to as a schema, and it

could be suggested that most participants had developed well-defined privacy schemas. Piaget theorised that cognitive schemas develop as a result of new challenges and opportunities being encountered, which may in turn be assimilated into existing schemas (Cherry, 2015b). Conversely, new experiences, influences, and information may challenge existing schemas and provide a catalyst for change and/or growth in long held schemas. Of interest are potential tensions that may arise between participants' privacy schemas and the affordances of new technologies introduced over time. Given participants' ease of interaction in and between online and offline contexts as seen in their responses, opportunities to interact in new ways with new technologies in the future may change how privacy is conceived, expressed and valued. Influences beyond participants' control related to the technologies themselves, modalities new technologies might offer, or limited technical capability to navigate these complexities, could provide the catalyst for new privacy schemas to evolve. These points provide a starting point for discussion and research in the future.

3.1 Influences in The Development of Participants' Privacy Concepts

The development of privacy concepts within an individual are determined in part by how and where one lives in the world (Kemp & Moore, 2007). As New Zealand has been described as having an individualistic culture (Smetana, 2010, p. 97), this implies that personal autonomy, rights of self, personal goals, independence, and self-reliance are valued and encouraged, in contrast to interdependence, collective goals, and national rights (Margulis, 2003; Smetana, 2010). Participants' desires and expressions of autonomy and control over their affairs and possessions, as well as their perceived personal rights, social negotiations of privacy and the desire for safety, suggest multiple representations of an individualistic culture. Where a nation's culture prioritises autonomy, personal rights and independence, it is more likely these values are encouraged by closer influences for example, family, through to broader influences such as legal systems. A few participants may have had some cognisance of legal rights, as

seen in comments pertaining to their rights of confidentiality of secrets and P.I; their control of disclosure of personal and family information; and expectations of freedom from being surveyed or stalked.

Cultural and social influences were also evident in the perceptions participants had pertaining to their need of privacy. Almost all participants considered their need of privacy to be similar or the same as their family and friends' needs. This was evident in data in which participants indicated on a scale their perceptions of privacy need, when comparing themselves to family, and then friends. A relationship is suggested between participants' value of privacy, and the similarity of privacy need with those closely connected to them. Thus, the social and cultural contexts in which participants and those closest to them cohabit and interact may help to sustain and foster similar privacy notions and behaviours.

Closer influences identified by participants in privacy development included family, school(s), peers, and other organisations. Participants' comments (40.0%) indicated that different family members had been instrumental in demonstrating, telling, or inadvertently role-modeling aspects of privacy importance and behaviours in everyday contexts. Brothers, sisters, and wider family helped some participants navigate privacy settings on SNSs and Apps. This is an encouraging finding, particularly in relation to the integral role that caregiver involvement and support performs in helping young people navigate the complexities of online environments, whether this be verbal or interactive mediation (Livingstone, 2008; Lwin, Stanaland, & Miyazaki, 2008; Strom & Strom, 2012). The immediacy, purpose, context, and interactions with others appeared to be determining factors in the privacy behaviours and privacy needs of many participants.

Schools, teachers, and educational resources were also influential and indicated in 19.0% of comments. It was unexpected that the influence of teachers, schools, and educational resources was more significant than peers' influence, which was only 13.0%. However, these findings align with other research that indicate schools can perform an effectual role in supporting young people to develop more robust media literacies and skills, enabling young people to manage themselves

confidently online (Liu et al., 2013; Lwin et al., 2008; McDonald-Brown, 2012). It is encouraging to see the role other people, organisations, media, and external structures had in helping shape values and behaviours of privacy in the lives of many participants, and were evident in 24.0% of comments. Examples of these included wider family, coaches, clubs, websites, police, church, Bible in Schools, television, and various experiences participants had encountered over time, and rules at school or in the home. These findings suggest there is value in encouraging young people to seek support from trusted others when needed, and this is encouraged widely on many online sites dedicated to the privacy and wellbeing of young people and their activities in online environments, for example Netsafe within the New Zealand context, and South West Grid for Learning Trust in the United Kingdom.

The wide-ranging privacy concepts and expressions of these across different contexts in participants' lives suggest degrees of maturity and competence in their understandings of the role privacy performs in their everyday lives. Further research into the privacy concepts of young people is recommended. This is particularly important in response to the scarcity of research and literature available on preteens' privacy concepts, privacy importance, influences, and examples in daily living in *offline* contexts in particular (West et al., 2009).

4. Devices and Underage Involvement on SNSs/Apps

Most participants indicated *they owned* more than one Internet-ready mobile device, and many (70.0%) also owned a computer, suggesting they potentially had mobility, autonomy, and choice of device. While most (87.0%) owned a tablet, iPad or iPod, over half owned a smartphone, which is consistent with other studies in comparative cultures (Lenhart, 2015; Macpherson, 2013; McDonald-Brown, 2012). The nature of learning and teaching in the New Zealand context sees many schools utilising mobile technologies in classrooms, which could account for the high number of participants having possession of one

or more devices. In addition, the desire or need for mobile communication between caregiver(s) and young people, has resulted in many young people having possession of a digital device that enables this connectivity.

Participants were aged between eleven and under thirteen years and all active (having a profile or account) on at least one SNS at the time of this study. This implicated participants as underage users on many SNSs carrying age restrictions of 13+ such as Facebook, Snapchat, Instagram, Kik, and Twitter. These age restrictions are a requirement by COPPA (Children's Online Privacy Protection Act) applied to American organisations to prevent commercial services being offered to those under 13 years, and to prevent collection of their P.I that may be used, on-sold, or released publicly (Children's Online Privacy Protection Act, 1998). By definition, participants should not have met the criteria required for this study. Furthermore, following full disclosure of the nature of the study, caregiver consent was required prior to participants' involvement. Thus, participants' caregivers were most likely aware of their underage activity on SNSs, and were unconcerned. This echoes in Strom and Strom's (2012) report related to underage SNS users which highlights the apparent unconcern of caregivers in regard to younger people's fabrication of age and participation on SNSs.

Studies exploring SNS use with younger audiences show that many users of SNSs are underage (McDonald-Brown, 2012), and of concern are reports that suggest usage of SNSs by both teens and younger children is increasing over time (EU Kids Online, 2014; Rideout et al., 2010). This is consistent with findings of this study in which most participants were between 10 and 12 years of age when creating their first SNS/App profile or account, while some were even younger. Most participants were either not aware of any age regulations on their SNSs/Apps, or were fully aware and undeterred by these requirements.

While these findings were not unexpected, the lack of awareness or care for any age restrictions applied to sites co-used by adults, poses concerns about the

apparent ambivalence of many participants. Similarly, the potential for participants to be exposed to adult themes and content through inadvertent or overt endeavour is of concern. The very nature of the Internet leans towards an absence of regulation, and embraces freedom of speech, liberal conduct, diverse and at times dangerous connections and networks, and spheres of content (Bartlett, 2014; boyd, 2014). Media frequently report potential online risks in association with harm, which is not founded on a reliable basis of research, and while such risks exist in this space, not all risks result in harm (Livingstone & Smith, 2014). However, other studies report that young people are not always aware of the complexities associated with challenges and risks to one's privacy, safety, and security online, and a potential negative bearing on one's wellbeing (NewsRx Health & Science, 2012; Yan, 2009).

This study inquired of participants' use, and preference of some age restricted (13+) SNSs, which are co-shared by adults and teens. Interestingly, findings indicated that Facebook was *not* the most prevalent, nor was it the most favoured SNS, which is at variance with other studies that indicate Facebook is still the most widely used SNS by adolescents across many countries (Crothers et al., 2013; Livingstone et al., 2013). Two other SNSs/Apps were shown to be more prevalent, and these were Snapchat, which 85.0% indicated they use and carries an age restriction of 13 years and over; and Instagram (82.0%), which carries an age restriction of 13 years and over. Again, these two favoured SNSs/Apps are co-used by adults and teens.

The underlying premise for underage SNS use, is the need to stay connected and visible with peers, and also the exploration of representations of self which are facets of one's evolving identity (O'Keeffe & Clarke-Pearson, 2011; Pascoe, 2008; Strom & Strom, 2012). This relates to the need to fit in with one's peer group(s) and these motivations strongly associate with identity formation of this adolescent age group as they explore, form, and present sometimes multiple projections of self across various social contexts (Livingstone, 2008). The finding that all participants were active on more than one SNS/App, suggests a

desire to connect and socialise with known and unknown others through various modalities provided by online SNSs/Apps and games.

Potential issues could arise as a result of participants who falsified their age information in order to create their accounts or profiles on SNSs/Apps (Livingstone et al., 2013). An example is Facebook, which 28.0% of participants indicated they used. This SNS provides an array of default privacy settings for users aged between 13-18 years which limits online audiences to 'friends only', and turns off the location settings (Facebook Help Center, 2015). However, if participants who used this SNS/App provided a birthdate that indicated they were over 18 years of age at the time of signing up, their privacy settings would have defaulted to the public domain unless manually changed. Furthermore, location services are automatically on, unless set otherwise. In other words, the global public could access everything some participants uploaded onto Facebook, and this content may have carried a location and time of upload. This also applies in instances of tagging names to images when uploaded by others. Also, all users on Facebook are purportedly 13 years of age and over, therefore all users' activities and content within this SNS can legally be tracked by Facebook, and information stored and used by third-party organisations. This in turn may mean that more adult themed advertising is displayed on a users' screen.

This example is similar to many other SNSs/Apps, however differences pertaining to their specific function may exist. Concerns related to age and fabrication of information arise, in that firstly there is a risk that norms may be developing that could see growing numbers of underage children using age restricted SNSs/Apps; secondly, as outlined in the example of Facebook, inherent risks associated with the fabrication of P.I needed to create an account on SNSs/Apps, may materialize (Skinner, 2010; Smith, 2015).

5. Caregiver Mediation and Oversight

Curiously, almost all participants perceived their caregivers to be highly familiar with their online activities. This is of interest, given that nearly half of (47.0%) respondents indicated that their caregiver(s) were essentially 'locked out' of

devices as they did not have the code or password to gain access. Furthermore, only a small percentage were linked in some way to participants' most prevalent and popular SNSs/Apps. For example, 14.0% were linked to participants' Facebook, 20.0% were linked to Instagram, and 10.0% were linked to Snapchat. Although 78.0% of participants indicated that their caregiver(s) were linked to one or more of their SNSs, this may be due to affordances of the technology to communicate and/or share content, or perhaps an intention to oversee online activity. However, reasons for this were not determined. Interestingly, some of these SNSs/Apps do not provide a means to share an account or profile, even if this was desirable. The extent to which this matters is a point for discussion, as many caregivers report they feel under-informed and overwhelmed with the task of supporting and supervising their children's online activities, especially on SNSs (Livingstone et al., 2013; O'Keeffe & Clarke-Pearson, 2011). Conversely, it could also suggest that some caregivers see this level of oversight or mediation as unnecessary or unethical.

A variety of strategies appeared to be undertaken by some caregivers in relation to oversight and/or mediation of participants' online activities. The most common strategy was the conveyance of appropriate types of ethical behaviour to be employed online, with just under a half of all respondents indicating these were expected of them, which was a positive finding. A few caregivers may have employed more restrictive strategies, such as allocating an amount of time and/or scheduling time when their child can participate online, and was evident in 23.0% of comments. In addition, a small group (7.0%) indicated that permission was required before using a device/SNS/App, and 5.0% shared that caregivers placed restrictions on where their device(s) were stored, particularly at night. Two participants reported that their caregivers had established rights to confiscate or remove devices/apps, and similarly, two indicated their caregivers had rights to view what they did online. Only three participants indicated their caregivers had restrictions or specifications on what SNSs/Apps were allowed, and three reported that homework or tasks had to be completed before they could use their devices. Most participants inferred that some agreement, rule, or strategy had been implemented in the home at some stage.

The conveyance of ethical and safe behaviours online by caregivers may have been underpinned by efforts to mitigate potential risks to their child's privacy and wellbeing, intentions that align with other studies (Hatch, 2011; Schofield Clark, 2011). This is also an encouraging finding, for other studies indicate that caregiver involvement is crucial in helping young people navigate the challenges, risks, and opportunities presented online (Valcke et al., 2010; Yardi & Bruckman, 2011).

6. Conduct, Contact, and Concerns Related to Devices and the Online Environment

In contrast to the mature privacy concepts and behaviours indicated in responses, inconsistencies emerged relating to the sharing of sensitive P.I, particular online activities, and access by others to some participants' devices. Of surprise was the large number (71.0%) who actively shared or used others' passwords, and over half (58.0%) reported they forget to sign out of online sites that require personal passwords. Furthermore, over half (58.0%) indicated they had shared their device, and some (45.0%) used others' devices. A smaller group (25.0%) had allowed others to change settings on their devices, and a few (8.0%) indicated they had changed settings on others' devices. There may be several factors to explain these actions and behaviours which are incongruent with privacy caution and care, and concerns related to these may indeed be unfounded. However, these practices appeared to rely on high degrees of trust of known and/or unknown others. An assumption of trust appeared to be made by these participants, that their device, P.I, or online content would be kept private and safe by those known to them who had access to it. Motivations for undertaking some of these risky actions seemed to overshadow notions of privacy, security and safety of one's online content and/or device(s). The underlying precept of creating passwords is the means to manage and restrict access of others to one's personal and private affairs, thus securing its safekeeping. The prevalence of sharing and/or using others' passwords suggests that benefits outweighed any perceived risks, and until a negative experience is incurred, it is possible these practices may continue (Lwin et al., 2012).

It was encouraging to see that many participants had utilized other tools and strategies enabling them to control others' access to their device(s) or online SNSs/Apps and content. This was seen in those who used eight character passwords (78.0%), those who had passwords or codes to access devices (83.0%), and those who used different passwords for different sites (40.0%). Also, a small number of participants indicated use of security tools such as virus protection, clearing of search History/Cookies online, and installation of an App to locate one's device if lost. These participants had at some point developed familiarity and technical competency with these tools, factors that potentially empower them in the management of aspects of their privacy and security in online environments. Of concern were those who indicated ambivalence or a lack of knowledge in knowing about or using specified tools that aid privacy and security of content and site information. An example is the use of privacy settings to select who can see your content, and over a third of responses indicated they did not know how, were not interested in knowing how, or knew but didn't bother to use these settings. This could suggest that those in this group were particularly vulnerable and potentially disempowered in the event of any online encounters that posed risks or concerns.

Reasons underlying the conflicting findings are not clear, and multiple factors may have underpinned these responses such as difficulties in navigating around complex interfaces of some SNSs/Apps in order to alter settings, reporting concerns to a site, or editing and deleting content (Christofides et al., 2012). It is also possible that pressure from peers is at times applied, when their passwords are forgotten, or not working, and it can be quicker and easier to use someone else's passwords to gain online access when needed or desired. Also, some may be motivated by the perceived benefits of allowing others to access one's accounts or devices to increase one's status both online, and offline. For example, a desire to gain further success on game levels can be achieved through allowing more skillful others to access their accounts and play on their behalf; or 'jail breaking' one's device by someone who knows how, to customise the interface and features which is currently a popular pursuit. These examples may be a factor in why some participants shared certain P.I, passwords, devices, or changed settings.

Concerns arise relating to possible types of harm some participants may incur in relation to online risks or challenges that may be precipitated through their lack of knowledge or technical skill. Similarly, those who were more ambivalent towards using online tools and mechanisms designed to support one's privacy and safety online, are of concern. It could be suggested that until an event or conflicting information presents a need for those participants to understand why and how to use mechanisms and strategies in the face of challenges, some participants' practices may not change.

6.1 Online Disclosure and Visibility of Personal Content

There was uncertainty by some participants in relation to which particular P.I was visible to the wider public in online environments. Also, in some instances there was a willingness to share pertinent P.I within this public domain. For example, half of all participants had a recognisable photo of themselves on their public profile(s) of SNSs/Apps, and others (20%) were unsure whether their photo was recognisable, or visible on their public profile. For some (23%) it appeared that sharing their school, sports club, or home address on SNSs/Apps as part of the visible profile, was of no particular concern. Others (18%) indicated they had shared their actual birthdate or phone number on public online profiles.

The extent to which these findings matter are a point for discussion, but concerns are raised simply by the lack of clarity that participants had in regard to visibility as well as the implications of the wider online public having access to pertinent P.I. De Souza and Dick (2009) state there is evidence that those children who value privacy in their daily lives are more likely to make careful judgments about disclosure of P.I online. Interestingly, the more one is visible online through sharing personal information and content as well as constructing one's online image in a positive light, the more they gain from this network exchange on SNSs/Apps, thus increasing one's status (De Souza & Dick, 2009). Therefore, underlying motivations can be a persuasive force in just how much and what one shares.

Other studies suggest that many young people have no clear boundaries on where the divide between public and private audiences lie, and that visibility is a particular pursuit of youth, enabled through the modalities of various online sites (Blatterer et al., 2010; West, Lewis, & Currie, 2009). However, Livingstone (2008) suggests not only are youth intensely interested in privacy, they are active in choosing public and private boundaries. In contrast to this view, participants' notions of what particular information or content was public or private were at times indistinguishable. This was evidenced in part in relation to online environments where P.I was required in order to create accounts and profiles on SNS/Apps. Some participants proffered truthful information in required 'boxes' or spaces, that were then made visible through the particular design interface. Inadvertent sharing of P.I was another issue whereby some participants lacked awareness or technical capability to control what they were sharing, and with whom.

Permissive access that some participants afforded to known and unknown others in online contexts, as well as the practice of sharing devices and having changes made to the settings on one's device, raises queries, and concerns. These concerns include firstly, preteens' need to understand degrees of visibility for differentiated audiences when sharing pertinent information online. Secondly, this vulnerable age group need to make considered and informed decisions relating to their devices and online activities. The findings suggest that knowledge of what comprises the 'public domain' is not clearly understood, and as participants indicated they value privacy, some might choose to change the visibility of certain P.I if they were more aware of potential risks and challenges associated with disclosure in the public domain online. Encouragingly, many participants did not share pertinent P.I publicly and many (83.0%) appeared to have a high level of awareness of how many 'friends' they had added to their profile(s). In addition, most (93.0%) indicated they had removed 'followers' and 'friends' from their online SNSs/Apps at some stage in the past. These findings may indicate that many participants actively controlled the status of their audiences, thus maintaining familiarity with their personal networks online.

A larger number of participants showed confident knowledge and capability in utilising tools, settings, and strategies available to them online and on device(s), which is encouraging. However, those whose knowledge and actions were less informed and/or competent were potentially susceptible to challenges and risks that could compromise their privacy and impact on their wellbeing. Interestingly, most participants perceived their capability in managing their privacy and any safety related issues online, as being relatively high, as indicated on the Likert Scale. With 7 marking the degree of capability as highly confident, skilled, and knowledgeable, 82.0% indicated they were at a 5, 6, or 7 on this scale. This suggests there is a divide between participants' perceptions related to disclosure of P.I online, and actual disclosure to various audiences, whether inadvertently or intended.

6.2 Online Conduct, Contact and Subsequent Concerns

Of importance were the types of online experiences, conduct, and/or contact that provoked degrees of concern in some participants, and any ensuing actions undertaken in response. Encouragingly, numbers of participants appeared to have no experience of the scenarios which included unknown persons making unwanted contact (40.0%); inappropriate conduct online (40.0%); loss of control of images or videos (26.0%); or viewing content that was offensive or concerning (63.0%). Almost half of all participants undertook actions to support others when online, who were the target of negative contact or conduct, which is an encouraging finding. Interestingly, a third of all participants had been involved in an emotive conflict online at some point, consistent with the belief that the nuances of offline relationships and networks are mirrored online (Hundley & Shyles, 2010). This is further suggested in the actions of a very small number (3.0%) who had willfully undertaken hurtful actions towards someone else online, and one who had pretended to be someone else online. The opportunity to 'hide' or 'project' one's self online is afforded by various online site modalities, and can be an advantageous option, but also carries risks. Of greater concern were those

responses (12.0%) that indicated a face-to-face meeting had occurred from contact made initially online. While this was not a common occurrence among participants and circumstances may have been risk-free, it is very concerning.

A relationship exists between the prevalence of disclosure of P.I online, negative experiences such as online bullying, and likelihood of engagement in risky behaviours such as meeting face to face with those met online (Lenhart, Madden, Smith, Purcell, Zickuhr, & Rainie, 2011). While few indicated they had engaged in these risky behaviours, concerns surface in relation to the wellbeing and safety of those individuals who had, and their ability to weigh opportunity against risk. Further complexities in privacy development and associated wellbeing, are evident in the levels of concern experienced by some participants (63.0%) in response to certain online conduct, contact or content. The ensuing actions of these participants could indicate that aspects of integrity, justice, peer pressure, or inner conflict underpinned their various concerns. Online conduct and contact can at times confront, challenge, or compromise users' privacy and boundaries, whether these encounters are directed specifically at a user, or through observing such encounters of behaviours happening to others. For example, some (8.0%) held degrees of concern in relation to people doing things online that weren't okay to someone else, but did not take any further action, and a small number (5.0%) indicated some concern regarding strangers making contact, and likewise, did not respond. Similarly, 5.0% reported considerable concern in others' uploading photos or videos in which they appeared, but had not undertaken any further action. Only a few (3.0%) indicated they had encountered disturbing content and did not respond in anyway.

How one is perceived by peers, and whether there is enough personal gain in responding to concerns encountered online, are factors that may have influenced the decisions of a few who had concerns, but did not choose to act on these. Young people are reticent in coming forward when encountering abusive contact or conduct that threaten or compromise their sense of safety, privacy, or self (Elgot, 2015), and are mirrored in these particular findings. A small number commented on what actions they undertook in response to concerns, however it

was encouraging to find some who perceived the need to do something. This was seen in those who told a caregiver or teacher (21.0%); spoke directly to the perpetrator (21.0%); reported conduct or activity to the site (12.0%); and those who blocked certain others online (30.0%). These actions reflect levels of technical competence and social confidence by those who executed the various responses.

The array of risks and challenges online are vast, and those which were of particular concern to some participants, are also common to other young people (Hundley & Shyles, 2010; Lazarinis, 2010; Valcke, Schellens, Keer, & Gerarts, 2007). These included swearing; hacking; unknown others making unwanted contact; known others uploading images or videos that included participants in them; and encountering disturbing content online. The most common experience was the observation of others who had uploaded cruel comments or content about others, with 21.0 % of participants indicating this. Of those (63.0%) who described their concerns encountered online, 35.0% reported teasing and nasty commenting as an issue. Participants' coping strategies, knowledge, and technical capability in using online security and privacy tools, may have been a factor in the ensuing actions some participants undertook in response to their concerns. It is not surprising that of those who responded, 30.0% had blocked others' access, while 12.0% reported concerning behaviours to the site administration, and 4.0% understood benefits in clearing their site History. These strategies suggest many had some knowledge and skill to use the tools purposed to manage their privacy, security and safety, and align with other teens' key response which is to block problematic others online (Hundley & Shyles, 2010; Lenhart et al., 2013a).

Encouragingly 21.0% of those who responded told others they trusted, and were primarily caregivers or teachers. Similarly, 21.0% communicated directly with a perpetrator to reinforce boundaries in relation to unwanted contact or conduct. Of particular worry was the description from one participant that self-harm had evolved and anxiety had developed, because of negative online encounters with both known and unknown others. This participant eventually sought support from their caregiver(s), and it appeared that some resolution had been achieved. The

impact of these events on the wellbeing of this participant was evident in the described actions of self-harming. Of further concern however, was the indication that they had continued to withhold information that online bullying had continued to be an issue. As a result of this particular disclosure, and my corresponding ethical responsibilities as the researcher, I met with the staff member who was responsible for assisting me in my research in this school, and described the key concerns. While it was not possible to confirm who the student was, it was decided that dedicated e-Safety and online citizenship class sessions would be undertaken, with a particular focus on resilience, options for action, and sharing issues with someone trusted. I was also assured that the School Counsellor, School Psychologist, and Head of this school, were to be advised. Communication later confirmed these steps had been undertaken.

In assessing whether to act on one's concerns, those participants who had encountered various disconcerting encounters online may have been swayed by perceptions of risks, perceptions of the event itself, or whether the perpetrator(s) were known to the participant. Even personal factors such as personality types could have been contributors (Liu et al., 2013). Furthermore, those who had some technical competency as well as supportive and sustained mediation provided by their caregiver(s), were more likely to execute appropriate and positive steps in managing challenges posed by online environments (Yan, 2006, 2009).

7. Inter-relatedness Between Preteens' Private Offline Self, Preteens' Online Self, and Influencing Factors

During the coding and analysis process, the findings indicated that cultural, social, and technical influences, as well as the technologies themselves are interrelated with preteens' concepts of privacy. These concepts also related to aspects of an 'offline private self' and an 'online private self', however, these appeared to be seamlessly linked at times. In response to these findings, I developed a simple model as I considered aspects of the inter-relatedness of the findings. I became aware that such a model could be used as a tool in future research to further examine the relationships that exist. Additionally, the degree to which the

relationships have an affect on preteens' concern for privacy in both offline and online contexts, could also be explored using this model. The model shown in Figure 1 is explained below.

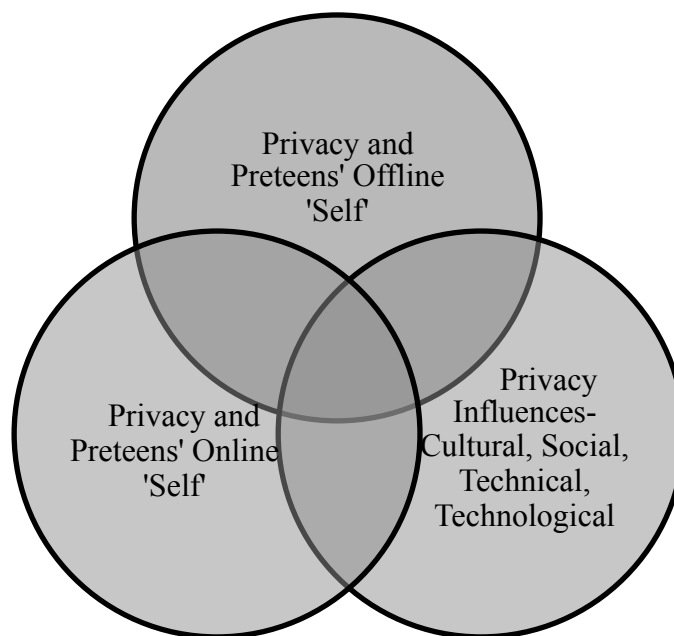


Figure 1. A model indicating the shifting relationships between preteens' private-self, contexts, and influences, in the development of privacy concepts and behaviours.

There may be potential for deeper consistencies to develop between preteens' privacy concepts and behaviours across contexts, and in relation to influences, and this potential is represented where all three spheres overlap. Further research is needed to explore the degree and nature of any intersections, and whether these lean towards a positive or negative positioning of privacy importance, and a concern for privacy. Further research using this model in interviews or focus groups could provide additional information for stakeholders, of the needs of preteens. Any further information may help to support the development of resilient and positive privacy concepts and behaviours, across online and offline contexts.

8. Summary

In summary, participants appeared to move between offline and online worlds with fluency, and while the findings indicated some participants had a relatively high awareness and consistency in some aspects of their privacy across both contexts, others did not. The strategies needed to protect one's privacy online have distinct differences to those offline. Also, one's evaluation of any risks associated with disclosure online may have been influenced by perceptions of benefits. Various groups of people and organisations appeared to provide positive support and influence in helping participants develop privacy behaviours and strategies, but not all are familiar or skilled in assisting them in the complexities of the online environment. While participants seem to be confident and skilled in negotiating many challenges presented online in regard to their privacy, concerns exist for those who lack technical skill, knowledge, and understandings to respond confidently to these challenges.

The complexities of online social interactions, the technology itself, and competing agencies such as organisational interests, are not considered to support or maintain stable and transparent practices online (Lazarinis, 2010; Livingstone, Ólafsson, & Staksrud, 2013). The implications of any instability or lack of transparency online suggest on-going challenges for participants and other young people, to confidently and skillfully execute independent judgment and control over personal contact and management of P.I online. Despite the apparent mature and insightful privacy concepts and practices of many participants, intentions to control and manage their privacy online could be impeded by the very nature of the Internet and many online sites. An interesting question is whether the desire or ability to control one's privacy might persist, as technological affordances keep evolving, and online sites continue to require crucial P.I while maintaining rights to use and on-share this P.I information with third party organisations. It requires users to be resolute in their diligence and scrutiny of their own sharing online, and also understanding the settings, terms, and privacy statements of their online SNSs/Apps. A model shown in Figure 1 illustrates the inter-relatedness of

influences and aspects of one's private self, online and offline, as indicated in the findings. It suggests that these three aspects are inter-related in varying degrees, and further research using this model may be beneficial in understanding young people and privacy in greater depth. Further recommendations are shared in the next chapter as conclusions are drawn from the findings and discussion.

Chapter Six: Conclusion, Implications and Recommendations

Introduction

This chapter summarises the most salient aspects of the study that have emerged. Implications of the research are described, and recommendations are made for caregivers, schools, and site administrators in helping young people navigate social and technical complexities in online environments. Limitations of the study are outlined, and potential benefits of further research in this area of study are discussed. The chapter concludes with a final statement.

1. Summary of the Study

This study sought to explore preteens' concepts of privacy and how these may have developed, and examined the nature of any relationships that may exist between these concepts and their behaviours and actions in online contexts. This section summarises the key aspects that emerged in relation to the research questions.

Those involved in this study primarily valued privacy, with many expressing robust concepts of what privacy is from their own perspectives and experiences. Many indicated an awareness of their rights to privacy and detailed privacy perspectives relating to aspects of self. Autonomy and control were important aspects of privacy, indicating growing maturity. Similarly, care and value of personal information, personal belongings, one's own space, and solitude were integral in privacy concepts. The perceived nature of relationships governed boundaries relating to ones' self and ones' possessions and others' access to these. Therefore, trust was an essential component in aspects of privacy. Physical privacy of the body and a sense of safety and security were also important concepts.

Some of these privacy values and concepts seamlessly crossed online and offline contexts, however inconsistencies in privacy behaviours and concepts were evident in some areas relating to online practices, and interactions with devices. Underlying factors that may have contributed to these inconsistencies included limitations in one's technical knowledge, a high degree of trust in others in relation to disclosure of personal information and sharing of devices, difficulties in managing socially complex situations online, and age-related maturity and limited experience.

The prevalence of access to more than one mobile Internet-connected device, and the high degree of perceived or actual ownership of these by preteens, suggested considerable autonomy in the use of devices and access to the Internet. This independence was evident in the prolific participation across multiple social network sites carrying age restrictions of 13 years and over and co-used by adults, from as young as ten years of age. Preteens also perceived that their caregivers had limited involvement with their online activities and devices, thus suggesting further opportunities for autonomous behaviour. While preteens indicated importance in the role that caregivers, schools, and peers had in supporting their understanding of complexities online, the methods and extent to which this occurred appeared to be irregular and the effectiveness was unknown.

The degree of concern for privacy is one of the key indicators of potential risky online behaviours, and encouragingly, many of those in this study appeared to have a healthy concern for privacy. While others had influential roles in shaping privacy values, many preteens undertook aspects of managing various technical, social, and ethical complexities online relying largely on the knowledge and values they had at the time. While many perceived themselves to be knowledgeable and confident about managing these aspects, this did not always equate to actual competencies required to cope with many of the technical and social complexities arising online.

2. Implications for Caregivers, Educators, Organisations, and Young People

The responsibility for helping young people develop a concern for privacy as well as competencies required in managing privacy online, lies foremost with caregivers who are legally tasked with the safety and wellbeing of their child, however schools are also expected to protect and care for the welfare of their students. In addition, issues related to students' social lives lived online often spill over into the school environment, thus social aspects become a school issue. Moreover, schools can place additional pressure on caregivers, with requirements for children to use devices and access the Internet as learning tools at school *and* home. Thus, schools are encouraged to develop and provide learning opportunities that include the technical competencies required to confidently manage online environments, as well as device knowledge. They also need to actively develop young people's understandings and social skills that in turn, may aid them in negotiating social complexities, privacy, and safety online. To ensure equity of learning opportunities in these areas for every young person within the New Zealand educational context, support and further structure is required.

This has implications on the Ministry of Education in relation to future policy and curriculum development, in that the current e-Learning Planning Framework document does not imply equity or relevance for all young learners in New Zealand. Many educators and trainee teachers may need further resources and professional development in order to provide the level of sustained, relevant, and age-appropriate learning opportunities required for young people in this area of learning.

Aspects of 'self' were encapsulated in preteens' privacy concepts and are integral in one's self-identity. The depth of their concepts indicated an importance in sourcing from young people themselves, the values, and behaviours they positively associate with privacy and privacy rights across domains. If educators and caregivers work *alongside* young people, drawing on *their* perspectives, this may in turn help them to build stronger links across contexts in which positive

concerns for privacy may deepen. Further research is needed to ascertain the benefits of a student-centered approach to linking privacy concepts and values more concretely in this way.

Those caregivers who feel overwhelmed and under informed of many technical and social aspects associated with their children's online activities, may feel ineffectual and worried by the potential risks the Internet and SNSs/Apps present, and as often amplified by media. While age restrictions that are applied to many online sites are a legal requirement in the U.S.A., caregiver familiarisation of those sites their children desire to use or are using, is recommended. Deepening the understanding of what may be a *potential* risk in contrast to an *actual* risk that incurs repercussions, may help caregivers develop further confidence in considering how to mitigate potential risks, yet still promote the opportunities of online social environments to their children.

The promotion of caregiver participation *alongside* their child may increase their technical knowledge, confidence, and efficacy related to various technologies. Additionally, while interacting in online environments alongside their child, new opportunities can occur between the technologies, the child, and caregiver, that may further develop relationships, deepen knowledge, and additionally, new content may be created. This may be particularly positive for those caregivers who perceive they are left out, that is, when caregivers believe that their child is more engaged with 'virtual others', and less 'in the moment' with those actually in the same physical space.

This suggests further support is needed to encourage and inform caregivers of the crucial role they perform in helping their children form positive concepts of privacy, and the uptake of these in their online and offline lives. To build greater trust and transparency in children's use of technologies and online environments, and to support their development of social and technical skills, active caregiver participation is recommended. This approach encourages a greater confidence and competency in managing some of the complexities with devices and online

environments for both the child, and the caregiver. Deepening partnerships between schools, home, and young people in sharing information, skills, and understandings related to privacy and wellbeing across contexts, is recommended.

Those responsible for the creation of online sites need to provide comprehensive and clear pathways that are easily navigated by users to control settings with ease, and understand the site terms and conditions of use with clarity. While there is pressure from lobbyist groups within some countries to further regulate aspects of site administration, regulation is a very complex and difficult endeavour with wide-reaching implications on areas such as laws, citizens' rights, and cultural considerations. Therefore, while there is a reliance on most site administrators to respond to this need for clearer navigation pathways, the response of any organisation is a social obligation, not a legal requirement at this stage.

Exercising control over boundaries related to access and permissions was an important aspect of privacy to almost all of those in this study. Young people are developing and experimenting with decision-making processes that are complex and inter-related with many aspects of self-identity, and external influences such as authority figures, peers, and culture. It is important that young people develop linkages between understanding privacy in offline and online contexts, and decisions made within these environments, and any potential implications of these. An example is the sharing of naked images via texts with another(s), often with the associated personal, social and/or legal risks and implications less considered or known. These include losing control of who has access to intimate images, or laws that prohibit the making, possessing, or distributing of images depicting any under-age (under 18 years) person(s) sexual parts or activity. Thus, young people need on-going access to relevant information across a range of issues relating to privacy, the Internet, and the social and legal implications associated with a range of online activities that carry potential risk.

As relationships with peers take on growing importance as children move into the preteen years, it is important that issues of trust are measured against the need for protection of privacy. Young people's perception of trust was intrinsic to their

levels of privacy behaviours in some settings, such as the prolific sharing of passwords with others, and similarly, the sharing of devices. However, as some relationships can be transient or changeable, young people need to develop intrinsic and ‘non-negotiable’ boundaries around the disclosure of certain private information or specific objects, barring exceptional circumstances and protocols within families and schools.

Becoming more literate of ownership of information, rights of users, responsibilities of site use, and knowing how to manage unwanted contact, inappropriate content, and act on concerns, are essential skills that young people need. It is recommended that young people become more familiar with aspects of the technical functions of their devices, and online tools and settings that enable privacy controls, editing options, and reporting tools that can be activated and managed. In addition, developing knowledge of the rights of the user *and* the site administrators and device brand in relation to how users’ information and content is stored and shared, is recommended.

3. Limitations of the Study

This small-scale qualitative study has some limitations. While undertaking the role of the researcher I was also known as a local teacher to some of the participants, which may have influenced some participants’ responses by adopting a ‘desired’ or ‘correct’ way of responding. This may have been further enforced through the ‘gate-keeper’ effect of having a supervising teacher present. While it was emphasised that responses were confidential, there was no right or wrong way to answer, nor were there expectations to answer in a certain way, the setting of the survey in a classroom and the presence of known supervising personnel may have influenced the authenticity of some participants’ responses.

All participants attended higher decile ranked schools and were all located in the same provincial city, which may have presented limitations to the study. Therefore, adopting a mixed-methods approach across a wider demographic may provide more detailed data and findings. This in turn may potentially offer more

in-depth perspectives from a greater number of young people that can be analysed and reported, allowing more comprehensive conclusions to be formed.

A focus group was included in the data-gathering methods, however the survey yielded more data than anticipated and was sufficient for the purpose of this thesis. While the data gathered through the focus group is intended to be used for future articles, the reliance on a single data set from the survey may be a limitation in this study.

Data was elicited from equal numbers of male and female participants. However, analysing any gender differences and presenting findings was not possible due to constraints of the size of this study. If this was possible, further conclusions may have been formed.

4. Areas for Future Research

Further research is recommended to enquire of the nature, quality, and frequency of support from the various groups identified as important by those in this study. In addition, it could be beneficial to find what competencies and literacies related to privacy and safety across contexts young people identify as essential. Drawing from the responses of young people themselves and using these to emphasise aspects that emerge such as resilience, citizenship, autonomy, and integrity, may in turn help put a positive spotlight on the capabilities of many young people, in contrast to the often negative attention generated through the media.

As participants indicated the important role that caregivers, educators, and schools have in shaping their concepts of privacy, future research could seek to explore what particular skills and strategies might be used to up-skill these particularly influential groups. Furthermore, inquiry into what learning resources and opportunities are available for students, caregivers, and educators, and the effectiveness of these, are examples of possible research in the future that could offer important information in this less researched area.

The model in Figure 1 that is described in the Discussion chapter could be used for further research into the inter-relatedness of influences, ones' private 'offline self', and ones' private 'online self'. This in turn, may provide deeper insights and outcomes into understanding the nature and degree of relationships between integral aspects. This could be particularly so if using a mixed methods data-gathering approach across a wide number of preteens and a broader demographic.

5. Conclusion

Literature and research relating to preteens' privacy focuses primarily on childhood development theories, or privacy related to online contexts. There appeared to be limited information relating to preteens' concepts of privacy and what value they associate with privacy in broader contexts. This was in contrast to the growing body of research associated with the online environment, its opportunities, challenges, and risks. This could imply that there are potential future opportunities to use the outcomes that emerged in this study in understanding this younger age group and their privacy concepts in *both* online and offline contexts. It could also be particularly beneficial for caregivers, educators, and schools in supporting younger people's knowledge and wellbeing, particularly as they learn, socialise and entertain within complex and challenging environments both offline *and* online.

While those in this study appeared to present mature and broad concepts of what privacy meant to them, some activities, behaviours, and decisions undertaken by some participants on digital devices, and in online social environments indicated inconsistencies with these concepts and values. Furthermore, particular decisions and actions some participants undertook, contradicted information of what is generally considered safe and appropriate when online, and on devices. This raises concerns and questions, and indicates there is much research and work to be done to understand complexities involved in these issues with young people.

Tailoring learning opportunities within curricula for young people is important and implications are drawn for policy makers and curriculum designers to consider what level of support might be needed to provide such resourcing. This includes the up-skilling of *every* educator as needed, to ensure all young people in New Zealand are given opportunities to develop competencies and skills required to confidently navigate online environments for learning and leisure. In conjunction, education resources tailored to meet student needs in this area need to be relevant, engaging, and accessible to all learners of all ages. Furthermore, learning opportunities need to be regular and sustained across the school year.

There are many influences involved in helping shape young people's privacy concepts and behaviours from the broadest contexts that include culture and environment, through to more personal and local factors such as family, schools, educators, and peers. The Internet itself is another factor providing its own complexities and opportunities for young people to navigate and form notions of the role of privacy in the open online environment.

In summary, the findings in this study support the literature that proposes young people can be resilient and resourceful. In addition, the findings provide *new* information related to young peoples' notions of privacy because of the scarcity of literature in that area. Therefore, I posit that if young people are provided with opportunities to determine and describe what privacy is, develop knowledge of privacy rights, *and* draw on their own privacy concepts and knowledge, it is possible that deeper links between privacy aspects across offline and online contexts could be forged. In turn, this may potentially serve to modify privacy schemas relating to self, privacy, security, and safety across contexts. Using the model in Figure 1 as a basis for future research, this may provide further insights into this less-researched area relating to privacy and younger people. In addition, further opportunities to inform caregivers, educators, and other stakeholders may emerge from additional research of young people's privacy perspectives, and how they may be given agency to integrate these more deeply into their learning and experiences across online and offline contexts. This suggests a greater partnership

is required between young people, caregivers, educators, government, content providers, and other organisations.

References

- Altman, I. (1977). Privacy regulation: Culturally universal or culturally specific? *Journal of Social Issues*, 33(3). <http://courses.cs.vt.edu/cs6204/Privacy-Security/Papers/Privacy/Privacy-Regulation.pdf>
- Awan, F., & Gauntlett, D. (2013). Young people's uses and understandings of online social networks in their everyday lives. *Young*, 21(2), 111–132. Retrieved from Sage Journals database.
- Bartlett, J. (2014). *The dark net*. London, United Kingdom: William Heinemann.
- Belsky, S. (2010). What happened to downtime? The extinction of deep thinking and sacred space. Retrieved from <http://www.fastcompany.com/1700298/what-happened-downtime-extinction-deep-thinking-and-sacred-space>
- Blatterer, H., Johnson, P., & Markus, M. R. (2010). *Modern privacy: Shifting boundaries, new forms*. Retrieved from ebrary database.
- boyd, d. (2014). *Its complicated: The social lives of networked teens*. London. United Kingdom: Yale University Press.
- Bratman, B. E. (2002). Brandeis and Warren's the right to privacy and the birth of the right to privacy. *Tennessee Law Review*, 69(3), 623. Retrieved from <http://heinonline.org>
- Brown, S. (2011, December). Social media: Friend or foe? *Momentum*, 42(4), 16–18. Retrieved from ProQuest Central database.
- Buckingham, D., & Willett, R. (Eds.). (2013). *Digital generations: Children, young people, and the new media*. Taylor and Francis. Retrieved from ebrary database.
- Burke, C. (2005). "Play in focus": Children researching their own spaces and places for play. *Children, Youth and Environments*, 15(1), 27–53. Retrieved from JSTOR database.

- Carson, J. (2007). Survey research with children. *Journal of Research in Nursing*, 12(5), 471–472. Retrieved from Sage Journals database.
- Check, J., & Schutt, R. K. (2012). *Research methods in education*. Los Angeles, CA: Sage Publications.
- Cherry, K. (2015a). How do children develop morality? Kohlberg's theory. Retrieved from <http://psychology.about.com/od/developmentalpsychology/a/kohlberg.htm>
- Cherry, K. (2015b). Piaget's stages of cognitive development. Retrieved from <http://psychology.about.com/od/piagetstheory/a/keyconcepts.htm>
- Children's Commissioner Act 2003, N.Z
- Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501-6505
- Christofides, E., Muise, A., & Desmarais, S. (2012). Risky disclosures on Facebook: The effect of having a bad experience on online behavior. *Journal of Adolescent Research*, 27(6), 714–731. <http://doi.org/10.1177/0743558411432635>
- Clark, A., & Moss, P. (2011). *Listening to young children: The mosaic approach* (2nd ed.). Retrieved from ebrary database.
- Cohen, L., Manion, L., & Morrison, K. (2007). *Research methods in education* (6th ed.). London, United Kingdom: Routledge Falmer.
- Cohen, L., Manion, L., & Morrison, K. (2011). *Research methods in education* (7th ed.). Taylor and Francis. Retrieved from ebrary database.
- Common Sense Media. (2015). Common Sense Media. Retrieved from <https://www.commonsensemedia.org/>
- Cox Communications. (2014). *2014 Teen Internet safety survey*. Retrieved from <http://www.cox.com/wcm/en/aboutus/datasheet/takecharge/tween-internet-safety-survey.pdf>

- Cranmer, S., Selwyn, N., & Potter, J. (2009). Exploring primary pupils' experiences and understandings of "e-safety". *Education and Information Technologies, 14*(2), 127–142. Retrieved from Springer database.
- Crothers, C., Gibson, A., Smith, P., Bell, A., & Miller, M. (2013). *World Internet project New Zealand: Internet trends in New Zealand 2007-2013*. Retrieved from http://www.aut.ac.nz/_data/assets/pdf_file/0005/473576/ONLINE-WIPNZ2007_20137_7-0702a.pdf
- Davidson, C., & Tolich, M. (Eds.). (2003). *Social science research in New Zealand: Many paths to understanding*. Auckland, New Zealand: Pearson Education.
- De Souza, Z., & Dick, G. N. (2009). Disclosure of information by children in social networking: Not just a case of "you show me yours and I'll show you mine." *International Journal of Information Management, 29*(4), 255–261. <http://doi.org/10.1016/j.ijinfomgt.2009.03.006>
- Drouin, M., Ross, J., & Tobin, E. (2015). Sexting: A new, digital vehicle for intimate partner aggression? *Computers in Human Behavior, 50*, 197–204. <http://doi.org/10.1016/j.chb.2015.04.001>
- Elgot, J. (2015). One in five young people has suffered online abuse, study finds. *The Guardian*. Retrieved from <http://www.theguardian.com/society/2015/sep/22/cyberbullying-teenagers-worse-than-drug-abuse-says-report>
- Erdur-Baker, Ö. (2010). Cyberbullying and its correlation to traditional bullying, gender and frequent and risky usage of Internet-mediated communication tools. *New Media & Society, 12*(1), 109–125. <http://doi.org/10.1177/1461444809341260>
- EU Kids Online. (2014). EU Kids Online: Findings, methods, recommendations. Retrieved from <http://eprints.lse.ac.uk/60512/>
- Facebook Help Center. (2015). Facebook help center. Retrieved from <https://www.facebook.com/help/473865172623776/>

- Finkelhor, D. (2014). Commentary: Cause for alarm? Youth and Internet risk research - a commentary on Livingstone and Smith (2014). *Journal of Child Psychology and Psychiatry*, 55(6).
<http://www.unh.edu/ccrc/pdf/CV315.pdf>
- Fowler, F. (1998). Design and evaluation of survey questions. In L. Bickman & D. Rog (Eds.), *Handbook of applied social research methods* (pp. 365–374). Thousand Oaks, CA: Sage Publications.
- Gibbs, J. C. (2013). *Moral development and reality: Beyond the theories of Kohlberg, Hoffman, and Haidt*. Retrieved from
<http://www.oxfordscholarship.com/view/10.1093/acprof:osobl/9780199976171.001.0001/acprof-9780199976171>
- Ginsburg, K. R., & Jablo, M. M. (2014). *Building resilience in children and teens: Giving kids roots and wings* (3rd ed.). Elk Grove Village, IL: American Academy of Pediatrics.
- Green, V. A., Harcourt, S., Mattioni, L., & Prior, T. (2013). *Bullying in New Zealand schools: A final report*. Wellington, New Zealand: Victoria University. Retrieved from www.victoria.ac.nz/education/pdf/Bullying-in-NZ-Schools.pdf
- Haduong, P. L., Wood, Z. E., Cortesi, S. C., Plunkett, L., Topelson, D., & Gasser, U. (2015). *Student privacy: The next frontier emerging & future privacy issues in K-12 learning environments* (Research Publication No. 2015-12). Berkman Center for Internet & Society at Harvard University. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2638022
- Hague, C., & Payton, S. (2010). Digital literacy across the curriculum. Futurelab Innovation in Education. Retrieved from
<http://archive.futurelab.org.uk/resources/publications-reports-articles/handbooks/Handbook1706>
- Harmful Digital Communications Act 2015, N.Z.
- Harter, S. (2012). *Construction of the self: Developmental and sociocultural foundations* (2nd ed.). Retrieved from ebrary database.

- Hart Research Associates. (2015). *Parents, privacy and technology use*. Washington, DC: Family Online Safety Institute. Retrieved from <https://www.fosi.org/policy-research/>
- Hatch, K. E. (2011). *Determining the effects of technology on children* (Senior Honors Projects). University of Rhode Island. Retrieved from <http://digitalcommons.uri.edu/srhonorsprog/260>
- Hawk, S. T., Keijsers, L., Hale 111, W. W., & Meeus, W. (2009). Mind your own business! Longitudinal relations between perceived privacy invasion and adolescent-parent conflict. *Journal of Family Psychology, 23*(4), 511–520. <http://doi.org/10.1037/a0015426>
- Hodkinson, P., & Lincoln, S. (2008). Online journals as virtual bedrooms? Young people, identity and personal space. *Young, 16*(1), 27–46. <http://doi.org/10.1177/110330880701600103>
- Hundley, H. L., & Shyles, L. (2010). U.S teenagers' perceptions and awareness of digital technology: a focus group approach. *New Media And Society, 12*(3), 417–433. <http://doi.org/10.1177/1461444809342558>
- Ihaka, J. (2008, July 10). Online bullying affects 1 in 3 children. *New Zealand Herald*. Retrieved from http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10520847
- Inness, J. (1992). *Privacy, intimacy, and isolation*. New York, NY: Oxford University Press.
- Ito, M., Horst, H., Bittanti, M., boyd, d., Herr-Stephenson, B., Lange, P. G., ... Robinson, L. (2008). Living and learning with new media: Summary of findings from the digital youth project. Retrieved from <http://digitalyouth.ischool.berkeley.edu/files/report/digitalyouth-WhitePaper.pdf>
- Jones, L. M., Mitchell, K. J., & Walsh, W. A. (2013). Evaluation of Internet child safety materials used by ICAC task forces in schools and community settings, final report? Retrieved from <https://www.ncjrs.gov/App/Publications/abstract.aspx?>

- Kafai, Y. B., Fields, D. A., & Ito, M. (2013). *Connected play: Tweens in a virtual world*. MIT Press. Retrieved from ebrary database.
- Kasper, D. V. S. (2005). The evolution (or devolution) of privacy. *Sociological Forum*, 20(1), 69–92. Retrieved from JSTOR database.
- Kemp, R., & Moore, A. D. (2007). Privacy. *Library Hi Tech*, 25(1), 58–78.
<http://doi.org/10.1108/07378830710735867>
- Lazarinis, F. (2010). Online risks obstructing safe Internet access for students. *The Electronic Library*, 28(1), 157–170.
<http://doi.org/10.1108/02640471011023441>
- Lenhart, A. (2015). Teens, social media & technology overview 2015. Retrieved from <http://www.pewinternet.org/2015/04/09/teens-social-media-technology-2015/>
- Lenhart, A., Madden, M., Cortesi, S., Gasser, U., & Smith, A. (2013a). Teens, social media, and privacy. Retrieved from <http://www.pewinternet.org/2013/08/15/where-teens-seek-online-privacy-advice/>
- Lenhart, A., Madden, M., Cortesi, S., Gasser, U., & Smith, A. (2013b). Where teens seek online privacy advice. Retrieved from <http://www.pewinternet.org/2013/08/15/where-teens-seek-online-privacy-advice/>
- Lenhart, A., Madden, M., Smith, A., Purcell, K., Zickuhr, K., & Rainie, L. (2011a). Teens, kindness and cruelty on social network sites: How American teens navigate the new world of “digital citizenship.” Retrieved from <http://www.pewinternet.org/2011/11/09/teens-kindness-and-cruelty-on-social-network-sites/>
- Lenhart, A., Madden, M., Smith, A., Purcell, K., Zickuhr, K., & Rainie, L. (2011b). Teens, kindness and cruelty on social network sites: Part 3: Privacy and safety issues. Retrieved from <http://www.pewinternet.org/2011/11/09/part-3-privacy-and-safety-issues/>
- Lewis, A., & Lindsay, G. (Eds.). (2000). *Researching children's perspectives*. Buckingham, UK: Open University Press.

- Lincoln, Y. S., Lynham, S. A., & Guba, E. G. (2005). Paradigmatic controversies, contradictions, and emerging confluences, revisited. In *N.K. Denzin & Y.S. Lincoln (Eds.), The SAGE handbook of qualitative research* (pp. 97–128). Los Angeles, CA: Sage Publications.
- Liu, C., Ang, R. P., & Lwin, M. O. (2013). Cognitive, personality, and social factors associated with adolescents' online personal information disclosure. *Journal of Adolescents*, *36*(4), 629–638.
<http://doi.org/10.1016/j.adolescence.2013.03.016>
- Livingstone, S. (2002). *Young people and new media: Childhood and the changing media environment*. Retrieved from ebrary database.
- Livingstone, S. (2008). Taking risky opportunities in youthful content creation: Teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media And Society*, *10*(3), 393–411.
<http://doi.org/10.1177/1461444808089415>
- Livingstone, S. (2013). Online risk, harm and vulnerability: Reflections on the evidence base for child Internet safety policy. *Zer*, *18*(35), 13–28.
<http://www.ehu.eus/zer/hemeroteca/pdfs/zer35-01-livingstone.pdf>
- Livingstone, S. (2014). *How children engage with the Internet*. Youtube.
Retrieved from
<https://www.youtube.com/watch?v=SyjbDUP1o0g&feature=youtu.be&list=PLVN0qOZiePqFEGAqE5md2bFQj75yVW7sp>
- Livingstone, S. (2015). As ever younger kids go online, how is the family responding? Retrieved from <http://clrn.dmlhub.net/content/as-ever-younger-kids-go-online-how-is-the-family-responding>
- Livingstone, S., Kirwil, L., Ponte, C., & Staksrud, E. (2014). In their own words: What bothers children online? *European Journal of Communication*, *29*(3), 271–288. Retrieved from Sage database.
- Livingstone, S., Ólafsson, K., & Staksrud, E. (2013). Risky social networking practices among “underage” users: Lessons for evidence-based policy. *Journal of Computer-Mediated Communication*, *18*(3), 303–320.
<http://doi.org/10.1111/jcc4.12012>

- Livingstone, S., & Smith, P. K. (2014). Annual research review: Harms experienced by child users of online and mobile technologies: The nature, prevalence and management of sexual and aggressive risks in the digital age. *Journal of Child Psychology and Psychiatry*, *55*(6), 635–654. <http://doi.org/10.1111/jcpp.12197>
- London School of Economics. (2015). Parenting for a digital future. Retrieved November 8, 2015, from <http://blogs.lse.ac.uk/parenting4digitalfuture/>
- Lwin, M. O., Miyazaki, A. D., Stanaland, A. J. S., & Lee, E. (2012). Online usage motive and information disclosure for preteen children. *Young Consumers*, *13*(4), 345–356. <http://doi.org/10.1108/17473611211282590>
- Lwin, M. O., Stanaland, A. J. S., & Miyazaki, A. D. (2008). Protecting children's privacy online: How parental mediation strategies affect website safeguard effectiveness. *Journal of Retailing*, *84*(2), 205–217. <http://doi.org/10.1016/j.jretai.2008.04.004>
- Macpherson, K. (2013). *Digital technology and Australian teenagers. Consumption, study and careers*. Retrieved from http://www.canberra.edu.au/researchrepository/file/fde6c9c8-0f73-47a6-afb2-e476699be44b/1/full_text_final.pdf
- Madden, M., Cortesi, S., Gasser, U., Lenhart, A., & Duggan, M. (2012). Parents, teens, and online privacy. Retrieved from <http://www.pewinternet.org/2012/11/20/parents-teens-and-online-privacy/>
- Magi, T. J. (2011). Fourteen reasons privacy matters: A multidisciplinary review of scholarly literature. *The Library Quarterly: Information, Community, Policy*, *81*(2). Retrieved from JSTOR database.
- Margulis, S. T. (2003). Privacy as a social issue and behavioral concept. *Journal of Social Issues*, *59*(2), 243–261. <http://doi.org/10.1111/1540-4560.00063>
- McDonald-Brown, C. I. L. (2012). *Kiwi kids online: An exploration of the contexts, challenges and competencies of pre-teenage children on the Internet*. Auckland University.
- McGlynn, A. P. (2010, July 12). Kaiser study shows media use by youth is heavy and rising. *The Hispanic Outlook in Higher Education*, *20*(19), 26–28. Retrieved from ProQuest Central database.

- McLeod, S. A. (2013). Erik Erikson. Retrieved July 21, 2015, from <http://www.simplypsychology.org/Erik-Erikson.html>
- Meadows, S. (1986). *Understanding child development*. Routledge. Retrieved from ebrary database.
- Meter, D. J., & Bauman, S. (2015). When sharing is a bad idea: The effects of online social network engagement and sharing passwords with friends on cyberbullying involvement. *Cyberpsychology, Behaviour, and Social Networking*, 18(8), 437–442. <http://doi.org/10.1089/cyber.2015.0081>
- Milosevic, T. (2015). E-Safety and education in the United States: What this means for parents. Retrieved from <http://blogs.lse.ac.uk/parenting4digitalfuture/2015/10/07/esafety-and-education-in-the-united-states-what-this-means-for-parents/>
- Ministry of Education. (2010). eLearning Planning Framework. New Zealand Ministry of Education. Retrieved from www.elearning.tki.org.nz/professional-learning
- Ministry of Education. (2015). The National Administration Guidelines (NAGs). Retrieved from <http://www.education.govt.nz/ministry-of-education/legislation/nags/#NAG5>
- Moshman, D. (2011). *Adolescent rationality and development: Cognition, morality, and identity* (3rd ed.). Retrieved from ebrary database.
- Mutch, C. (2013). *Doing educational research. A practitioner's guide to getting started*. (2nd ed.). Wellington, New Zealand: NZCER Press.
- NewsRx Health & Science. (2012). Bullying; Expanded study will track adolescent behavior on Facebook. *NewsRx Health & Science*. Retrieved from ProQuest Central database.
- Novakovic, L., McGill, T., & Dixon, M. (2009). Understanding user behavior towards passwords through acceptance and use modeling. *International Journal of Information Security and Privacy*, 3(1), 11–29. Retrieved from ProQuest Central database.

- Ofcom. (2015). Children's media lives: Year 1 findings. Ofcom. Retrieved from <http://stakeholders.ofcom.org.uk/>
- Ohler, J. (2012). Character education for the digital age. *The Education Digest*, 77(8), 4–17. Retrieved from ProQuest Central database.
- O'Keeffe, G. S., & Clarke-Pearson, K. (2011). The impact of social media on children, adolescents, and families. *Pediatrics*, 127(4), 800–804. <http://doi.org/10.1542/peds.2011-0054>
- Ontario Ministry of Education. (2015). Literacy for a connected world. Retrieved from <http://find.gov.on.ca/?searchType=simple&owner=edu&url=&collection=educationtcu&offset=0&lang=en&type=ANY&q=Digital+literacies+cyber+safety>
- Parke, R. D., & Sawin, D. B. (1979). Children's privacy in the home: Developmental, ecological, and child-rearing determinants. *Environment and Behaviour*, 11(1), 87–104. <http://doi.org/10.1177/0013916579111004>
- Parker, R. B. (1974). A definition of privacy. *Rutgers Law Review*, 27, 275–296. Retrieved from HeinOnline Law journal Library database.
- Pascoe, C. J. (2008, January 22). Living digital: teens and technology. Retrieved from <http://www.pbs.org/wgbh/pages/frontline/kidsonline/interviews/pascoe.html>
- Peterson, A. (2015, November 2). Snapchat's new terms of service freaked people out because no one reads them. *The Washington Post*. Retrieved from <https://www.washingtonpost.com/news/the-switch/wp/2015/11/02/snapchats-new-terms-of-service-freaked-people-out-because-no-one-reads-them/>
- Pilger, J. (2013). WikiLeaks is a rare truth-teller. Smearing Julian Assange is shameful. *New Statesman*, 142(5145), 42–42. Retrieved from EBSCO database.
- preteen. (2015). In *Oxford Dictionary of English* (3rd ed.). Retrieved from <http://www.oxforddictionaries.com/definition/english/pre-teen>

- Rainie, L., Lenhart, A., & Smith, A. (2012). The tone of life on social networking sites. Retrieved from <http://www.pewinternet.org/2012/02/09/the-tone-of-life-on-social-networking-sites/>
- Reed, E. S., Turiel, E., & Brown, T. (2013). *Jean Piaget symposia series: Values and knowledge*. Psychology Press. Retrieved from ebrary database.
- Rideout, V. J., Foehr, U. G., & Roberts, D. F. (2010). *Generation m2: Media in the lives of 8- to 18 year olds*. Retrieved from <https://kaiserfamilyfoundation.files.wordpress.com/2013/04/8010.pdf>
- Sapsford, R. (2007). *Survey Research* (2nd ed.). London, United Kingdom: Sage Publications.
- Schoeman, F. (2008). *Privacy and social freedom*. Cambridge: Cambridge University Press.
- Schofield Clark, L. (2011). Parental mediation theory for the digital age. *Communication Theory*, 21(4), 323–343. <http://doi.org/10.1111/j.1468-2885.2011.01391.x>
- Shmuell, B., & Blecher-Prigat, A. (2011). Privacy for children. *Columbia Human Rights Law Review*, 42(3), 759–795. <http://heinonline.org>
- Skinner, C. (2010). 4 out of 5 parents let children use Facebook. Retrieved from <http://www.networkworld.com/article/2241022/collaboration-social/4-out-of-5-parents-let-children-use-facebook.html>
- Smetana, J. G. (2010). *Adolescents, families, and social development: How teens construct their worlds*. Retrieved from ebrary database.
- Smith, L. (2015). Is Kik messenger safe for kids? Retrieved from <http://theyybersafetylady.com.au/2013/07/why-kik-messenger-is-unsafe-for-kids/>
- Solove, D. J. (2002). Conceptualizing privacy. *California Law Review*, 90, 1087–1155. <http://doi.org/10.2307/3481326>

- Spielhagen, F. R., & Schwartz, P. D. (Eds.). (2013). *Adolescence in the 21st century: Constants and challenges*. Information Age Publishing. Retrieved from ebrary database.
- Sticks'n'stones. (2016). Sticks'n'stones. Retrieved from <http://www.sticksnstones.co.nz/>
- Strom, P., & Strom, R. (2012). Growing up with social networks and online communities. *The Education Digest*, 78(1), 48–51. Retrieved from ProQuest Central database.
- Tinson, J. (2009). *Conduction research with children and adolescents: Design, methods and empirical cases*. Mesa, AZ: Goodfellow Publishers Limited.
- Trepte, S., & Reinecke, L. (2011). *Privacy online: Perspectives on privacy and self-disclosure in the social web*. Springer Science & Business Media. Retrieved from ebrary database.
- Turkle, S. (2011). *Alone together: Why we expect from more technology and less from each other*. New York, NY: Basic Books.
- Valcke, M., Bonte, S., De Weaver, B., & Rots, I. (2010). Internet parenting styles and the impact on Internet use of primary school children. *Computers and Education*, 55, 454–464. <http://doi.org/10.1016/j.compedu.2010.02.009>
- Valcke, M., Schellens, T., Keer, H. V., & Gerarts, M. (2007). Primary school children's safe and unsafe use of the Internet and at school: An exploratory study. *Computers in Human Behavior*, 23(6), 2838–2850. <http://doi.org/10.1016/j.chb.2006.05.008>
- Vodafone New Zealand. (2016). Digi-Parenting: Age Guides. Retrieved from <https://digi-parenting.co.nz/digi-savvy-parenting/age-guides/>
- Waikato University. (2008). Ethical conduct in human research and related activities regulations. Retrieved from <http://calendar.waikato.ac.nz/assessment/ethicalConduct.html>
- West, A., Lewis, J., & Currie, P. (2009). Students' Facebook "friends": Public and private spheres. *Journal of Youth Studies*, 12(6), 615–627. <http://doi.org/10.1080/13676260902960752>

- Westin, A. F. (1967). *Privacy and freedom*. New York, NY: Atheneum.
- Yan, Z. (2005). Age differences in children's understanding of the complexity of the Internet. *Applied Psychology, 26*, 385–396.
<http://doi.org/10.1016/j.appdev.2005.04.001>
- Yan, Z. (2006). What influences children's and adolescents' understanding of the complexity of the Internet? *Developmental Psychology, 42*(3), 418–428.
<http://doi.org/10.1037/0012-1649.42.3.418>
- Yan, Z. (2009). Limited knowledge and limited resources: Children's and adolescents' understanding of the Internet. *Journal of Applied Developmental Psychology, 30*(2), 103–115.
<http://doi.org/10.1016/j.appdev.2008.10.012>
- Yardi, S., & Bruckman, A. (2011). Social and technical challenges in parenting teens' social media use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 3237–3246).
<http://doi.org/10.1145/1978942.1979422>
- Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviours among young adolescents. *Journal of Consumer Affairs, 43*(3), 389–418. <http://doi.org/10.1111/j.1745-6606.2009.01146.x>
- Younger, S. (2015). Interview with Dr. Michele Borba on parenting tweens. Retrieved from <http://www.chicagonow.com/tween-us/2015/07/dr-michele-borba-on-parenting-tweens/>

Appendices

Appendix A: Preteens and Privacy Survey

This survey is about your thoughts and ideas regarding privacy in different kinds of situations. Your responses are confidential. Your honest and full answers will be very valuable to the research I am doing. You are one of 60 students participating. If there is anything you find confusing, or you have any questions, please put up your hand and someone will come to you. If for any reason you wish to stop participating in the survey, please let your teacher or myself know. There is a 'SUBMIT' button at the end of the survey when you are ready to finish.

1. Indicate your gender
 - Female
 - Male

2. Indicate your age – are you between:
 - 11-12
 - 12-13

Your Ideas About Privacy – Section One

3. What is 'privacy' or 'having privacy'?

4. Show on the scale how privacy is or is not important to you.
[1= Not important at all; 7= Extremely Important]

5. List up to five examples where privacy has some personal importance to you.

6. What are your thoughts about privacy? (Tick all that apply)
 - I like privacy when I open mail/emails
 - I like privacy when I am on the home phone/cell phone

- I like private space away from family
- I am happy to share my belongings with others
- I don't really like sharing my belongings with others
- I don't mind others seeing my screen when I am online
- I do mind others seeing my screen when I am online
- I have given out personal information to unknown others
- I never give out personal information to unknown others

7. From a very early age, you have been developing ideas about privacy and practices of privacy. What and/or who may have influenced your ideas? (e.g. people, experiences, rules, organisations)

8. How important is your *need of privacy*, compared to your parent(s) or caregivers? Indicate your response.

(e.g. privacy of space, belongings, personal information)

[1= Less important; 7= More Important]

9. How important is your *need of privacy*, compared to your friends?

Indicate your response. (e.g. privacy of space, belongings, personal information)

[1= Less Important; 7= More Important]

Online Activities, Decision, and Tools

This section asks about the devices you use, and about being online, and what happens in this online space.

10. How do you go online? (Tick all that apply)

- I have my own smartphone
- I have my own tablet, iPad, iPod
- I have my own computer
- I share a smartphone
- I share a tablet, iPad, iPod
- I use other wi-fi or Bluetooth technology (t.v. etc)

11. What online social apps or sites do you use? (Tick all that apply)

- Facebook
- Instagram
- Facetime
- Twitter
- Snapchat
- Skype
- Kik
- Tumblr
- Ask.fm
- Youtube
- iMessenger
- Other

12. What is your favourite online social network app/site?

13. How much time would you spend on this site/app on average in one week?

14. When did you first create your profile/account on this app/site?

15. Do you know if there is an age restriction on this site/app?

(e.g. R13 or other?)

16. Are your parent(s)/caregiver able to see your activities online through friendship/linked accounts or profiles? (e.g. 'friend' on Facebook)

- None of my sites/apps
- One of my sites/apps
- More than one of my sites/apps

17. List which ones if you answered 'one' or 'some' in the question above.

18. Does your parent(s)/caregiver know what you mostly do online? Indicate your response.

[1= Not At All; 7= Mostly All]

19. My parent(s)/caregiver can...

(Mark only one)

- Access my device(s) without any password
- Access my device(s) with a known password
- Only access my device(s) if I put in my private password

20. On my device(s) I use the following security tools:

(Tick all that apply)

- A password or code protection on the screen
- Find my iPad/iPhone app installed
- Timer that locks screen
- Finger scanner
- Power Down or Sleep mode
- Firewall/Anti-virus/Anti-malware etc software
- Logging out of sites I use passwords for
- Clearing History/Cookies regularly
- Passwords that are at least 8 characters long
- Different passwords for different sites/apps

21. Have you done the following before:

(Tick all that apply)

- Let a friend take away or use my device(s)
- Used or taken away a friend(s) device
- Changed settings on someone else's device
- Had my settings changed on my device by a friend
- None of the above

22. Are there any rules or agreements by parent(s)/caregiver around the use of your device? (e.g. where, when, how it is used, what is okay, etc)

23. Do you know the following about your profile/account on a social network app/site? (Select Yes/No/Not Sure)

- Is there a recognisable photo of yourself on your public profile?
- Is your real birthdate showing on your public profile?
- Is your phone number listed on your public profile?
- Is your school, home address, sport or other club showing on your public profile?
- Do you know how many ‘friends’, ‘followers’, or contacts you have on your site approximately?
- Have you deleted any ‘friends’ or ‘followers’, or contacts on your sites/apps before?

24. Have you experienced the following online?

Mark only one oval per row. (No experience of this)

(Yes, but I wasn't really concerned) (Yes I was concerned)

(Yes I was really concerned but didn't do anything about it)

(Yes I was really concerned and I did something about it)

- People I don't know trying to connect with me
- People I don't know saying untrue things about me
- People I know saying untrue things about me
- People doing things online that aren't okay to others
- Photos/videos of me on others' sites/apps/phone
- Seeing content that was disturbing or inappropriate

25. Share what the nature of the event was that caused you concern and what you did or didn't do about it – if you marked any of the ‘concerned’ options above.

26. Personal information and online tools. Select the following that apply to activities online. Check all that apply.

- I've given my password out to a friend(s) before
- I've used someone else's password before
- I've given truthful information about myself to others I've never met before
- I don't mind my information/photos/videos being seen by anyone
- I forget to sign out from sites/apps and email sometimes
- I've asked someone else to delete a comment/photo/video that I was in, but didn't like
- None of the above

27. I know the rights (Terms and agreements) of the social network sites I use regarding my information and how it is used. [1=Not at all; 7=Fully understand]

28. Do you do the following online: Select one that best applies to you.

Mark only one oval. (Yes, when necessary) (I would, but don't know how) (I'm not interested in knowing) (No. I know how but don't bother)

- Clear recent searches/cookies
- Edit-delete post/photos/videos
- Use privacy settings to select who sees my posts/information
- Find out about the terms and agreements of how my information is stored and used
- Report to the site owners when I see anything wrong or concerning
- Delete or deactivate an account/profile

29. Your actions online: Have you...(Select those that apply)

- Defended/helped someone being targeted online
- Pretended to be someone else online
- Been involved in some kind of drama/argument/fight online
- Said/done hurtful things to someone else online before
- Met up (face to face) with someone you met online
- None of the above

30. Rate your confidence, skills, and knowledge in managing your privacy and safety online.

[1=not confident, skilled or knowledgeable; 7=Highly confident, skilled and knowledgeable]

Thank you for your participation and effort today in answering the survey questions. Your feedback is important and valuable. Your responses are confidential. If you are confident and comfortable with your responses and agree to submit your answers, please click on the SUBMIT button below.

SUBMIT

Appendix B: Mapping of Survey Questions

	Preteens' Concepts	Preteens' Decisions and Actions	Gender and Age	Table
Section One				
Privacy Concepts, Perceptions, Development, and Perceived Influences	Q.3		Q.1	T.2
	Q.4		Q.2	
	Q.5			
	Q.6			T.3
	Q.7			T.4
	Q.8			T.5
	Q.9			
Section Two				
Digital Devices, Age Restriction Awareness, Social Network Sites, and Caregiver Oversight	Q.11	Q.10		T.6
	Q.14	Q.11		T.7
	Q.16	Q.12		T.8
	Q.17	Q.14		T.9
	Q.19	Q.15		T.10
		Q.16		T.11
		Q.17		
		Q.19		
Online Privacy, Safety and Security, Tools and Settings	Q.21	Q.20		T.12
	Q.22	Q.21		T.13
	Q.23	Q.22		T.14
	Q.25	Q.23		T.15
	Q.26	Q.25		T.16
	Q.27	Q.26		T.17
	Q.29	Q.27		T.18
	Q.31	Q.29		T.19
		Q.30		T.20
Online Decisions, Experiences, Influences, and Ownership of Personal Information, Perceptions of Competency	Q.18	Q.18		T.12
	Q.23	Q.23		T.13
	Q.25	Q.25		T.14
	Q.26	Q.26		T.15
	Q.27	Q.27		T.16
	Q.29	Q.29		T.17
	Q.30	Q.30		T.18
				T.19

Appendix C: Survey Procedure Script

Hi my name is Angela Webster and as part of my university study, I am undertaking research, looking into young people's ideas about privacy in general, and how these ideas or concepts might have developed. This is covered in the first section of the survey. Also, I'm interested in young people's experiences and thoughts related to privacy, when using digital devices, and in online social network sites, and this is covered in the second part of the survey.

Your participation is really appreciated, and by being here today, I understand that you are volunteering to take part. If, for any reason, you don't want to complete the survey, or you are uncertain about the survey, that is okay. All you need to do is put your hand up and your teacher or myself will come over and have a quick chat, and you can exit out of the online survey form if you want to. If you have any questions during the survey, or are unsure of what a question is asking, please put your hand up and we will come to you. There are different ways to respond to some questions, and some will ask you to write your own words down, while others are multi-choice, or ranking questions. Take your time, there is no hurry, no prize for the first finished.

It's important for you to know that your answers or 'responses' as they're called, are all confidential. I am the only one who can read your responses, and there is no email address attached to them, so this means your school, your teacher, your parents, and myself – will have no way of linking anyone's responses to their name. I will only know which school the responses are from because of the particular date stamp on the survey. I appreciate you giving your time to provide confidential, honest, and full responses to the different questions, as this will help me understand young people's ideas about privacy.

When I have finished my study, I will write up a summary of what I find, and share these with each school. When you're happy with your responses, please finish by clicking on 'Submit'. Read or work quietly until everyone is finished, then I have something to give you, to say 'Thank You'.

Appendix D: Study Overview and Introduction Note to Caregivers

Angela Webster has been teaching at xxxxxx School for the last eleven years and is undertaking her Masters in Education full time this year. Angela has undertaken workshops with xxxxxx students and parents in discussing aspects of life online, and managing risks while seizing the opportunities these technologies offer. She is undertaking research required for her Masters thesis at three schools in the district. Her research will require 20 Year 8 students from each of the participating schools to complete an online survey and possible participation in a focus group.

The survey will be undertaken at school on a scheduled date for approximately 45 minutes. The focus group will be hosted at xxxxxxxxx School for a group of 6 students from the three schools, for approximately 45 mins. Her research will eventually provide a summary that will be shared with each participating school. Students are randomly selected based on a criteria that includes having access to an Internet-connected device, and active on at least one online social network site.

Personal information about your child's responses will be kept confidential under the requirements of the University of Waikato Ethics Committee.

We have given Angela our support and believe that her research will benefit parent and school communities as she furthers her knowledge and understandings of children's privacy concepts, resilience, and management in evolving and complex digital and online environments.

Please read, sign and return the attached Parent Consent form that is required for your child to participate in this research. It is encouraged for you to discuss aspects of the study with your child to ensure their participation is voluntary.

Kind regards

xxxxxxx

xxxxxxx School

Appendix E: Parental Information and Consent Form

March 2nd 2015

Mob: xxx xxxx xxx

Email: xxxxxxxxxxxxxx

Dear Parents and Caregivers

My name is Angela Webster and I am currently studying towards my Masters in Education, through Waikato University.

As part of this study, I am researching the perceptions and development of privacy in preteens, and how these may relate to their activities and decisions made in online environments, and on devices. I am sending you this letter to seek permission for your child to participate in the study.

The title of the study is: Preteens' concepts and development of privacy, and the relationship to decisions and actions undertaken in online social environments and with digital devices.

The study focuses on these key questions:

1. What are preteens' concepts of privacy, and how might these have developed?
2. What is the relationship to actions and decisions undertaken in online social environments and with digital devices?

Foci relating to these questions include:

1. Explore preteens' (11- < 13 years) concepts of what *privacy* is to them;
2. Find out what awareness preteens have of online *strategies/tools* that can support privacy;
3. Explore the *depth of knowledge* preteens might have regarding online settings and tools available to support privacy;

4. Explore the value preteens may attach to *personal information* and any constraints towards sharing this online;
5. Examine preteens' *understandings* of what can happen to their personal information on popular online sites.

If you agree to your child participating, the research will require one or both of the following activities:

1. An online Survey of no longer than 60 minutes and overseen by a supervising teacher and myself.
2. A follow up Focus group to be held at xxxxxx School for no longer than sixty minutes and facilitated by myself.

Student and school names will be kept confidential and only pseudonyms used in any reporting. However, complete anonymity cannot be guaranteed. Information collected from your child relating to the questions and foci above will be analysed alongside all students' data, and findings will be reported back as a summary to your school Principal. Outcomes from the study will be shared in my thesis, and other possible forums such as conferences, conference papers, publications, and online education forums. It is hoped that the results from this study could provide useful insights to help shape future thinking and planning for schools, caregivers, and students within the New Zealand education context.

I hope your child is able to participate in this study. Please discuss the nature of the research, and the opportunity to voluntarily participate in this research, with your child, as their willing participation is an important factor in the research process. If you do agree to their participation, please indicate consent on the attached form and return it to school. If you have any further questions relating to any aspect of the study, please do not hesitate to contact me using the details below.

Kind regards

(Signature)

Contact information:

Mob: xxxxxxxxxxxx

Email: xxxxxxxxxxxxxxxx

This study met the approval from the Ethics Committee of Waikato University in January 2015 (Serial Number EDU 112/14).

 Research Return Form (Parents/Caregivers)

Study Focus: Preteens' concepts and development of privacy, and the relationship to decisions and actions undertaken in online social environments and with digital devices.

I have read the information sheet regarding the research planned to be undertaken at my child's school. I give consent for my child to participate in the online Survey and Focus Group for the research purposes as outlined in the letter (Please tick).

Data may be collected from my child via the completion of the online Survey

Data may be collected from my child via Focus Group participation

I understand that data from the research may be used in a thesis, presentations, publications and other possible forums as outlined in the letter. If I have any questions or concerns, or wish to withdraw my child from the study, I can contact the researcher at any time.

Parent/Caregiver(s) Name:

Student Name:

School:

Date:

Appendix F: Head of School and Supervising Teacher Information and Participation Consent Form

School Leader and Supervising Teacher Information and participant Agreement.

Preteens' concepts and development of privacy, and the relationship to decisions and actions undertaken in online social environments and with digital devices.

Dear xxxxxx

My name is Angela Webster and I am currently studying towards my Masters in Education, through Waikato University. As part of this study, I am researching the concepts and development of privacy in preteens, and how/if these relate to their activities and decisions made in an online environment and with digital devices.

The study focuses on these key questions:

1. What are preteens' concepts of privacy, and how might these have developed?
2. What are the relationships to actions and decisions undertaken in complex online social environments and with digital devices?

Foci relating to these questions include:

1. Explore preteens' (11- < 13 years) concepts of what *privacy* is to them;
2. Find out what awareness preteens have of online *strategies/tools* that can support privacy;
3. Explore the *depth of knowledge* preteens might have regarding online settings and tools available to support privacy;

4. Explore the value preteens may attach to *personal information* and any constraints towards sharing this online;
5. Examine preteens' *understandings* of what can happen to their personal information on popular online sites.

If you agree to participation, the research will require the following activities:

1. An online Survey for 20 students aged between 11- < 13 years to be completed on a set date, for a duration of no longer than 60 minutes and overseen by myself as the researcher, and a supervising teacher.
2. A follow up Focus group to be held at xxxxxx School on a set date; two students who participated in the online Survey would participate in a discussion group for no longer than 60 minutes, facilitated by myself.
3. Enabling data collected from your students relating to the questions and foci above to be analysed, and findings to be reported through a thesis, and other possible forums such as conferences, conference papers, publications, online education forums. Student and school names will be kept confidential and only pseudonyms used in any reporting. However, complete anonymity cannot be guaranteed. It is anticipated that results from this study could provide useful insights to help shape future thinking and planning for schools, parents, and students in your school and possibly within the New Zealand education context.

I hope you agree to your school and students' participation in this study. If you do agree to this, please indicate consent on the attached form, keep a copy for yourself, and return the original to me. If you have any further questions relating to any aspect of the study, please do not hesitate to contact me using the details below.

Kind regards
Angela Webster
(Signature)

Contact information:

Mob: xxx xxxxxxxx

Email: xxxxxxxxxxxx

This study met the approval from the Ethics Committee of Waikato University in January 2015 (Serial Number EDU 112/14).

Research Return Form for Leaders of Schools and Supervising Teacher(s)

Preteens' concepts and development of privacy, and the relationship to decisions and actions undertaken on devices, and in online social environments.

I have read the information sheet and understand the nature of the research and what is required of the school and students involved. I permit the school and students to participate in it. (Please indicate in the boxes)

1. Data may be collected from students in our school via an online Survey.
2. Data may be collected from students in our school via a Focus Group.
3. Data may be analysed and findings reported for the purposes outlined, including publications or presentations.
4. I agree as Head of School/ Supervising Teacher

If I have any concerns, questions, or wish to withdraw myself, any student, or the school from the research, I may contact the researcher at any time.

Head of School name:

Supervising Teacher's name:

Signed:

Date