Drawing the line: Understanding privacy concern, privacy literacy and trust influences on online social network privacy boundaries

By Roberta Morrison

The University of Strathclyde
Department of Marketing

Submitted in accordance with the requirements for the degree of Doctor of Philosophy.

2013

This thesis is the result of the author's original research. It has been composed by the author and has not been previously submitted for examination which has led to the award of a degree.

Signed: B Morrison Date: Sept. 20, 2013

Acknowledgements

Completing this doctoral dissertation has been a defining experience that enabled me to learn more than I ever anticipated the process would offer. I certainly learned more about the topic of interest and more about the research process but I also learned so much about myself and the generosity of others. For, without the guidance, support and encouragement of so many, this thesis would not have been possible.

I would first like to thank my thesis supervisor, Prof. Alan Wilson, for his patience and leadership in seeing this project to completion. His wisdom and direction were invaluable inputs into both the process and final product and I am grateful to have learned so much under his supervision. I would also like to thank Dr. Michael Harker for his time and contributions to my Thesis Committee meetings and Dr. Stephen Tagg, convenor of the Committee.

The support of St. Francis Xavier University and so many of the faculty within the Schwartz School of Business were instrumental in my completion of this thesis as well. This endeavour could not have been pursued without the funding support provided from the St. FX Morley Chair and my initial endorsement from the Department of Business Administration under Chair, Dr. Tim Hynes. I am also deeply indebted to Dr. Todd Boyle who gave so freely of his time, advice and resources and Dr. Tom Mahaffey, without whose enthusiasm, encouragement and flexibility I may not have made it through. The understanding and support provided by Dr. Monica Diochon and Dean Leo Gallant as I juggled employment responsibilities with this research were also critical elements to the completion of

this project. I am also greatly appreciative for Nicole Mclean's tireless editorial assistance. And, I am grateful to the numerous other St.FX faculty who helped in a variety of capacities from contributing advice, encouragement, and their empathetic ears: Dr. Denton Anthony, Dr. Gabrielle Durepos, Mr. Randy Delorey, Dr. Brad Long, Dr. Ken MacAulay, Dr. Neil Maltby, and Dr. Mary Oxner.

Of course, without the participation of survey respondents, there would be no results to analyse or insights to provide. To all those who took the time out of their busy schedules to contribute to the data collection process, I am especially thankful.

Though I mention them last, their contribution to this project has not been a minor one. My family has lived this process too and have been my most powerful motivation and greatest enablers. I sincerely thank my thoughtful and selfless partner, Matt Gunning, who has picked up my slack without ever being asked, endured each frustration along this road and still found the strength to encourage me through. I am also especially grateful for the cheerleading offered by my children and extremely proud of their maturity to understand the team effort required to complete this thesis. My 'task-master' son, Gavin, kept me accountable for my productivity and the eternal positivity from my daughter, Lauren, made me a believer. Special thanks are also due to my sister, Dawn, who generously played second-mom beautifully and seamlessly and to my parents, Mike and Josephine, who supported this exercise from the outset, provided the confidence to make it to the end and helped in other innumerable practical ways.

Abstract

At the time of this research, online social network (OSN) participation was approaching ubiquity in the Western world. Online social network participation requires information disclosure to achieve social capital benefit, yet privacy concerns are commonly acknowledged among participants. Thus, understanding how information disclosures in OSNs are rationalised in light of privacy concerns is the topic of this this research. While some research into the privacy calculus has been accumulated in the literature, a complete understanding of the phenomenon is lacking. As a result, this research sought to provide novel explanations of the privacy paradox.

From a positivist perspective an embedded mixed methods research design was employed. Qualitative data was collected via focus groups to enrich and pre-test the survey instrument comprised of 12 latent constructs reflected by 82 manifest variables. A cross-sectional survey of 835 Canadian online social network users was subsequently conducted using a snowball sampling technique. The hypothesised measurement and structural model was analysed via Partial Least Squares Structural Equation Modelling techniques using SmartPLS 2.0.

Results of the measurement and structural models offered external validation of a commonly accepted privacy concern construct. Communication Privacy Management theory was found to offer an effective description of certain OSN behaviours, but the measurement structure of the construct was not observed as hypothesised. Yet, numerous findings about how communication privacy management functioned within the privacy calculus were concluded from this research. Of particular note were the significant influences of privacy literacy and trust in various stakeholders upon communication privacy boundary coordination. Trust in the OSN provider was singled out as a major influence on OSN behaviours. Objective privacy knowledge was confirmed to be low. Privacy concern was revealed to be higher than anticipated but its effect on the privacy calculus was not as important as the other constructs. Thus, results of the final model contributed a novel privacy calculus model argued to contribute to the explanation of the privacy paradox.

Among the original contributions of this research were the inclusion of a number of previously untested realtionships and constructs. Though theoretical support guided their inclusion, empirical tests of objective and subjective knowledge, trust in close connections and Communication Privacy Management had not previously been tested in the context of a privacy calculus in OSNs. Distinctions between the roles of both interpersonal and organisational trust were also evidenced.

Implications to the science of marketing were clear as this study offered an obvious extension of knowledge and opportunities for future research were identified. Implications to government were revealed as a result of findings about objective knowledge. Implications to practice included recommendations for continued emphasis upon trust development and improvement and attention to privacy awareness.

Table of Contents

List of Figures

List of Tables

Abbreviations and Symbols

APCO	Antecedent – Privacy Concern – Outcome
AST	Atlantic Standard Time
AVE	Average Variance Extracted
Avg	Average
B2C	Business-to-consumer
BL	Boundary Linkages
BP	Boundary Permeability
BPMM	Blogging Privacy Management Measure
BO	Boundary Ownership
C	Collection
CB-SEM	Covariance Based Structural Equation Modeling
CFA	Confirmatory Factor Analysis
CFIP	Concern for Information Privacy
CPM	Communication Privacy Management
CR	Composite Reliability
CRM	Customer Relationship Management
E	Errors
EFA	Exploratory Factor Analysis
GIPC	Global Information Privacy Concern
H	Hypothesis
IA	Improper Access
ICTs	Information Communication Technologies
IUIPC	Internet User Information Privacy Concern
MAU	Monthly Active User
NS	Not Significant
NSA	National Security Agency
OECD	Organisation for Economic and Co-Operative Development
OK	Objective Knowledge
OLS	Ordinary Least Squares
OPC	Office of the Privacy Commissioner
OSN	Online Social Network
OSN CPM	Online Social Network Communication Privacy Management
PETs	Privacy Enhancing Technologies
PCIA	Privacy Concern about Information Abuse
PCIF	Privacy Concern about Information Finding
PIPEDA	Personal Information and Protection of Electronic Documents Act
PLS	Partial Least Squares
PLS-SEM	Partial Least Squares Structural Equation Modeling
PRE	Power Responsibility Equilibrium
Q	Question
SCRM	Social Customer Relationship Management
SEM	Structural Equation Modeling
SK	Subjective Knowledge
SNS	Social Networks
S-O-R	Stimulus-Organism-Response

TAM	Trust in All Members
TCC	Trust in Close Connections
TP	Trust in Provider
U&G	Uses and Gratifications
UK	United Kingdom
US	United States
USU	Unauthorised Secondary Use
WEIRD	Western, Educated, Industrialized, Rich, and Democratic

α	Alpha
β	Path coefficient
F^2	Effect Size
M	Mean
N	Sample size
√	Square Root
t	statistical t value
p	statistical significance
R^2	Coefficient of Determination

1 Introduction

There has been a perplexing phenomenon observed within online social networks that this research aims to investigate. While online social networks (OSNs) are ideal environments for facilitating information exchange among individuals to create social benefits, the information that is exchanged to achieve those benefits also makes an individuals' information privacy vulnerable. Individuals acknowledge their concern for information privacy when polled, yet participation (and therefore information sharing) in OSNs has been uninhibited. This counterintuitive behaviour has been referred to as a privacy paradox and provides the impetus of this investigation. In efforts to explain the privacy paradox, various privacy calculi have been proposed in the literature. While a body of knowledge is being built to understand the phenomenon, there are still unresolved gaps in the literature. Thus, this research seeks to add to the understanding of the privacy calculus by testing relationships that have not yet been investigated or confidently determined in order to inform marketing science, business and government.

1.1 Study Rationale

Technology has allowed governments, business organisations and individuals to collect masses of consumer data. Bricks-and-mortar retailers track purchase behaviour with loyalty cards, online transactions and websites visited by an individual can be monitored and credit card companies mine scores of data relating to a variety of purchases and credit history. There are video surveillance cameras in hotels, financial institutions, retail stores, parking lots, transportation terminals and on many city streets. Electronic key cards that record time of entry and exit are commonly used to access parking garages, hotel rooms and office buildings. In addition, smartphones can pinpoint an individual's location (The Canadian Press, 2011) and biometric scanners are being used with increasing frequency (Singer, 2012). The ubiquity of smart phone cameras allows individuals to capture video anytime and anywhere (Saint Louis, 2011). And, the proliferation social media including online social networks (OSNs) allows the public sharing of user-generated content rife with intimate personal information.

These technological innovations have provided numerous benefits to interested parties. Companies desire vast quantities of consumer data to analyse and understand consumers so that they may engage in mutually beneficial long-term relationships. Government often requires substantial personal data for security reasons. And, individuals participate in online social networks for a variety of social benefits (i.e. Acquisti and Gross, 2006; Boyd, 2007; Joinson, 2008; Steinfield, Ellison and Lampe, 2008; Pfeil, Arjan and Zaphiris, 2009; Valenzuela, Park and Kim, 2009).

However, just as the dawn of instantaneous photographic technology called attention to privacy concerns in the late 1800s (Warren and Brandeis, 1890), technological evolution continues to challenge our notions of and attitudes toward privacy. Indeed, the public regularly associates privacy concerns with twenty-first century technologies (i.e. Westin 2003; Statistics Canada, 2010; Harris Decima, 2011). But, digital information communication technologies (ICTs), in particular, can alter both the nature of information privacy and our understanding of it (Floridi,

2005) and reveal unanticipated privacy harms (Solove, 2006; Cavoukian and Cameron, 2011). Particularly, within Web 2.0 environments where there is increased ease of combining data from multiple sources to create extensive consumer profiles unbeknownst to the individual (Nissenbaum, 2010; Cavoukian and Cameron, 2011; Kosinski, Stillwell, and Graepel, 2013; Naughton, 2013), there is the possibility that the privacy concerns individuals cite do not even reflect the full extent of the vulnerability associated with voluntary information disclosure in these contexts. Accordingly, one type of digital ICT – the online social network (OSN) - was thought to have its own set of privacy challenges given the unique way in which information is disclosed and therefore provides the context of this study.

Online social networks (OSNs) are user-generated online communities in which software facilitates joining people for a common purpose (Preece and Maloney-Krichmar, 2006) and social relationships with other online participants are enabled through non-private discussions (Brown, Broderick and Lee, 2007). These environments, which include Facebook, Twitter and LinkedIn, have become increasingly popular with most Internet users in Western nations participating (eMarketer, 2012; Ofcom, 2012; Oliveira, 2012).

What makes the issue of privacy particularly unique in OSN environments is the distinct way in which information is disclosed[1]. With many other forms of consumer data collection (i.e. loyalty card transaction behaviour or surveillance video), the consumer does not actively participate in the information disclosure, nor is the disclosure usually made to an audience. For example, although a consumer

[1] Self-disclosure is referred to herein according to the broad definition of the term articulated by Houghton et al (2013) which states that self-disclosure is “information intentionally communicated about person A to any person(s) via any form of communication and interaction by person A” (p.7).

may actively enrol in a loyalty card program, the data collection that occurs each time a transaction is made and the loyalty card swiped is imperceptible to the consumer. In contrast, OSNs members actively and publicly communicate certain personal information to register their account, make and articulate connections with other individuals and then publicly disclose various pieces of personal information to various audience members as frequently as they desire. To be sure, OSN providers also collect 'behind-the-scenes' data such as click-history from its members (Consumer Reports, 2012), but the repeated, voluntary and active disclosure of information by participants creates an interesting environment in which to investigate privacy. In addition, the presence of others modifies typical personal information disclosure environments. While a member may intend to share certain information with connections in their network, that information may also be publicly disclosed beyond their network depending upon the privacy settings selected or shared further by their own connections (Consumer Reports, 2012). Furthermore, the OSN provider is also a recipient of the disclosed information and other third party businesses with which the OSN provider has sharing agreements can constitute yet another audience.

Given the unique context of information disclosure in OSNs, the uncertainty associated with new technological environments, and the associated privacy concern cited in public opinion polls, it might be expected that individuals would be hesitant to share personal information in these environments. However, not only is OSN participation reaching a point of arguable ubiquity, information sharing on OSNs appears uninhibited (Acquisti and Gross, 2006; Huffman, 2013) in spite of stated privacy concerns. This counterintuitive phenomenon has been coined the 'privacy paradox' (Norberg, Horne and Horne, 2007) and is what this study intends to investigate.

1.2 Research Objectives

The natural question, then, is why do individuals continue to share their personal information in OSNs in spite of recognised privacy concerns? Thus, the primary research question guiding this study has been: *how can the privacy paradox be explained?*

Based on the notion that many people are 'privacy pragmatists' willing to trade-off some information privacy in exchange for benefits (Westin, 2003), research into the privacy calculus (Gross and Acquisti, 2005) has established that individuals do make certain rationalised choices about the risks and rewards associated with their personal information. Yet, as the literature review presented in Chapters 2 and 3 will elucidate, there are still numerous gaps in our understanding of the privacy calculus. Therefore, in seeking an answer to the research question, this study aims to extend the privacy literature by providing additional insight into online social network information disclosure decisions by testing relationships that have not previously been explored.

Accordingly, there were four main research objectives of this Project:

1. To validate a prominent conceptualization of privacy concern in the context of online social networks

2. To explain personal information disclosure in online social networks using Communication Privacy Management theory

3. To explain the role of privacy literacy in influencing online social network information disclosure decisions, and
4. To establish the role of trust in consumer information disclosure behaviours in online social networks.

In so doing, this study is intended to offer important contributions to three stakeholder groups – academia, business and government. Specifically, advancement in consumer privacy theory is expected to be achieved through insights offered from empirical tests of new constructs and relationships hypothesised to affect information disclosures in online social networks.

Businesses, particularly those that operate OSNs, are also expected to find the consumer insights generated to be of relevance, for understanding consumers is paramount to the relationship marketing paradigm commonly acknowledged to be so important (Grönroos, 1994). Third party businesses that utilise OSNs to connect with consumers should also find the results relevant for similar consumer insight and relationship management reasons, especially as these organisations strive to harness the power of social networks (Meyerson, 2010) and translate traditional customer relationship management (CRM) knowledge and practices to the social sphere with SCRM (Archer-Brown, Piercy and Joinson, 2013).

Finally, government is anticipated to be a beneficiary of the knowledge derived from this analysis as well. Governments worldwide, particularly those within the OECD (Organisation for Economic Co-Operative Development) have demonstrated great interest in privacy through the adoption of Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data beginning in 1980 and the enactment of various privacy legislation among independent member nations over the last 30 years (OECD, 2011). Each of these protections was designed to provide reasonable safeguards to citizens' privacy in an environment of escalating data collection consistent with the rapid technological evolution currently underway. Therefore, insight into individuals' privacy related attitudes and behaviours in privacy-vulnerable environments should complement the interests of government as they strive to protect citizen information privacy.

1.3 Research Approach

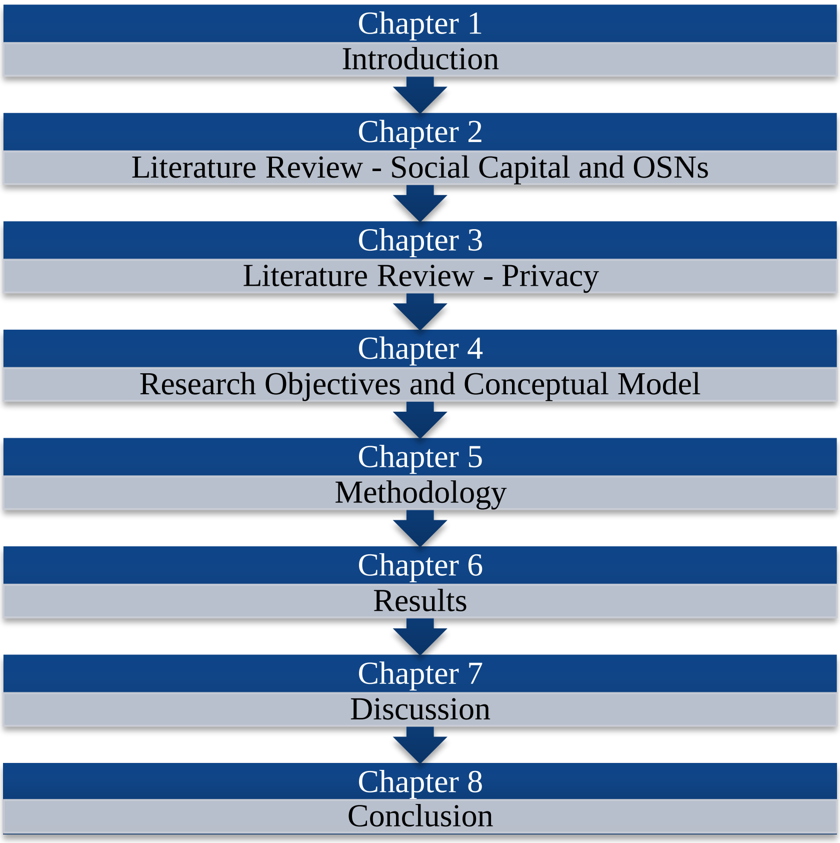
A positivist philosophical approach guides this research. Accordingly, a hypothetico-deductive approach will be used (Easterby-Smith et al, 2002). Positivist approaches frequently result in quantitative methods (Burrell and Morgan 1979; Kinnear and Taylor 1996; Easterby-Smith et al, 2002; Perri 6 and Bellamy 2012), though the use of qualitative techniques is not precluded (Crabtree et al 1993; Wolff, Knodel and Sittitrai, 1993; Bryman and Bell, 2003). Consequently, an 'embedded instrument development' research design involving mixed methods will be employed (Creswell and Plano Clark, 2011). Specifically, focus groups will be used as a supplemental qualitative strand of data collection intended to develop and refine pre-existing survey instruments within a dominant quantitative cross-sectional survey method approach.

After pilot testing the final survey instrument, data will be collected by a cross-sectional online survey hosted by the subscription software, Fluidsurveys.com, and incentivized via entry into a random draw for an iPad2. A purposive snowball sampling technique (Davidson 2006) will be used due to the lack of sampling frame available for online social network users (Adams, Khan and Raeside, 2007). Data collected will then be analysed using Partial Least Squares structural equation modelling techniques using SmartPLS 2.0 (Ringle, Wende, and Will, 2005) and both measurement model and conceptual structural models will be evaluated, refined as necessary, and re-evaluated to identify a statistically and theoretically acceptable final model.

1.4 Thesis Layout

The organisation of this thesis is as presented in Figure 1.1.

Figure 1.1 Thesis Layout



Following this introduction, the literature is reviewed in Chapter 2 and Chapter 3. Chapter 2 presents an overview of the context of the Project. It begins with a discussion of social capital theory and proceeds to introduce online social networks including the relevance of social capital theory to these environments. Chapter 3 discusses privacy through examination of the philosophical nature of the construct, identifies some of the definitional contention with the construct, presents the foundation of the research – the privacy paradox – and ultimately establishes a number of knowledge gaps with respect to available privacy calculus models intended to explain the privacy paradox.

Chapter 4 presents the research question and specific objectives developed from a number of knowledge gaps emerging from privacy calculus models presented in the literature. Each of those gaps is discussed in this chapter to justify the conceptual model to be tested in this study.

Chapter 5 discusses the research method employed beginning with the researcher's philosophical orientation to the problem. The research design is also detailed and characteristics of the sample are provided.

Chapter 6 presents the results of the research. The descriptive results are presented first followed by results of a PLS-SEM analysis conducted via SmartPLS 2.0 (Ringle, Wende, and Will, 2005).

Chapter 7 provides a discussion of the results. First, the findings from analysis of the measurement model are interpreted. Next, the analysis of the hypothesized structural model is discussed. Model re-specification, guided by both theory and statistical tests conducted herein, is justified prior to a presentation of the final model validated by the analysis.

Chapter 8 contains the conclusion of the research. In this chapter the contributions of the research are summarized, limitations of the work are identified and implications to science of marketing, business and government are surmised.

2 Social Capital and Online Social Networks

2.1 Social Capital

Social capital is generally explained as "the information, trust, and norms of reciprocity inhering in one's social networks" (Woolcock 1998, p.153), or the goodwill resultant from social relations (Adler and Kwon 2002, p.17). It has variously been defined in terms of trust, civic engagement, life satisfaction and social networks (Valenzuela, Park and Kim, 2009), though expressed most simply, social capital refers to the actual and potential resources available to people through their network of social connections (Coleman 1988; Nahapiet and Goshal 1998; Valenzuela, Park and Kim 2009). The resources typically related to social capital include information, emotional support, and an ability to organize social groups (Paxton 1999) and expectations of reciprocity (Valenzuela et al 2009). In addition to the term 'social capital' a variety of other terminology has alternatively been used to describe ideas of social capital including 'intangible assets', 'social energy', 'social capability', 'sociability', 'moral resources', 'ties' and 'networks' (Woolcock, 1998).

The term 'social capital' has been used in a variety of disciplines. Woolcock (1998) identified several substantive fields of social capital research including: i) families and youth behaviour problems, ii) schooling and education, iii) community life including both physical and virtual communities, iv) work and organisations, v) democracy and governance, and vi) general cases of collective action problems. Consequently, social capital has been recognized as an umbrella concept (Adler and

Kwon 2002) that is “close to becoming a joint concept for all social sciences” (Paldam 2000, p.631).

Like financial capital, physical capital and human capital, social capital has value in use (Nahapiet and Ghoshal, 1998) and facilitates productive activity (Coleman, 1988; Lin, Cook and Burt, 2001). Similarly, like other forms of capital, social capital is appropriable (Coleman 1988; Sandefur and Laumann 1998). Just as one might acquire physical capital for one purpose and subsequently use that physical capital in a capacity not originally anticipated, one can do the same with social capital. Accordingly, Coleman (1988) suggested that the social capital within a set of social relations might be appropriated to aid in another context. This means, for example, that one could accumulate social capital among social relations established via joint participation in a community volunteer group and then draw upon that resource to help identify employment opportunities or serve as a personal reference. And, like physical and human capital, social capital requires maintenance (Adler and Kwon, 2002). Social bonds require investments of time and attention or else they lose efficacy.

However, unlike other forms of capital, social capital cannot be independently owned by any one party due to its dependence upon social relationships (Burt, 1992). Social capital is the least tangible type of capital and does not reside within a tool of production or an individual themselves (Coleman, 1988). Instead, social capital “exists in the *relations* among persons” (Coleman, 1988, p.S100-1), thus, the resource is jointly owned by the parties in the relationship (Burt, 1992) and cannot be easily traded (Nahapiet and Ghoshal 1998).

While there is a general acceptance of the social capital construct, nuanced definitions have been made explicit in the literature. Thus, as the variety of definitions presented in Table 2.1 illustrates, ‘no simple definition exists’ (Leonard, 2004). A number of definitions of the construct presented in Table 2.1 illustrated that social capital was likely a multidimensional construct (Woolcock, 1998; Paldam, 2000; Scheufele and Shah, 2000). Indeed, Paldam (2000) offered five separate definitions of the construct, suggesting that social capital could be viewed in a variety of ways ranging from cooperation, trust, networks and consequences (trust payoff and network payoff). Further, authors that did not explicitly argue for the construct’s multidimensionality recognised or referred to other constructs in its definition. For example, Adler and Kwon (2002) stated that social capital brings together concepts of trust, culture, social resources, embeddedness, relational contracts, interfirm networks, informal organization and social networks.

A cursory review of these definitions (Table 2.1) did also suggest some commonalities, however. Specifically, social structures and relationships appear integral to the nature of social capital (Bourdieu, 1986; Coleman, 1988; Burt, 1992; Putnam, 1995; Nahapiet and Ghoshal, 1998; Portes, 1998; Paldam, 2000; Scheufele and Shah, 2000; Adler and Kwon, 2002). The centrality of trust to the concept of social capital was also clearly indicated by these definitions (Putnam, 1995, 2000; Fukuyama, 1995; Paldam, 2000; and Scheufele and Shah, 2000). And, while some authors have avoided the explicit use of ‘trust’ in their definition of the construct, a proximal relationship has been argued. For instance, Coleman (1988) asserted that social capital is dependent upon the “trustworthiness of the social environment” (p. S102).

Table 2.1 Definitions of Social Capital

Author	**Social Capital Definition**
Bourdieu (1986)	• “the aggregate of the actual or potential resources which are linked to a possession of a durable network of more or less institutionalized relationships of mutual acquaintance or recognition” (p.248) • “made up of social obligations (‘connections’) which is convertible, in certain conditions, into economic capital” (p.243)
Coleman (1988)	• “Social capital is defined by its function. It is not a single entity, but a variety of different entities having two things in common: they all consist of some aspect of social structures, and they facilitate certain actions of actors – whether persons or corporate actors – within the structure” (p. S98)
Burt (1992)	• “friends, colleagues, and more general contacts through whom you receive opportunities to use your financial and human capital” (p.9)
Woolcock (1998)	• “different conceptualizations suggest that there may be various forms or dimensions of social capital.” (p.156) • There are “four distinct dimensions of social capital - integration and linkage at the micro level, integrity and synergy at the macro level” (p.170)
Putnam (1995a, 2000)	• “"social capital" refers to features of social organization such as networks, norms, and social trust that facilitate coordination and cooperation for mutual benefit” (1995, p.66) • “trust and engagement are two underlying facets of the same underlying factor – social capital” (1995, p.73) • “connections among individuals – social networks and the norms of reciprocity and trustworthiness that arise from them” (2000, p. 19)
Fukuyama (1995)	• “Social capital is a capability that arises from the prevalence of trust in a society or in certain parts of it.” (p.26)
Nahapiet and Ghoshal (1998)	• “the sum of the actual and potential resources embedded within, available through, and derived from the network of relationships possessed by an individual or social unit” (p.243)
Portes (1998)	• “the ability of actors to secure benefits by virtue of membership in social networks or other social structures” (p. 6)
Paldam (2000)	• *Ease of cooperation definition:* social capital is the ability of a person to work voluntarily together with others for a common purpose (p. 635) • *Trust definition:* social capital is the quantity of trust a person has in other members. Trust is likely to be reciprocal so the trust a person has to everybody else corresponds to the trust they have to a person. The latter concept is sometimes known as a person’s goodwill. (p.635) • *Trust payoff definition:* social capital is the amount of benefits an individual can draw his goodwill. (p.635) • *Network definition:* social capital is a measure of the amount of networks a person has built. (p.641) • *Network payoff definition:* the social capital of a person is the total amount of benefits the person can draw on his network(s) if necessary. (p.641)
Scheufele and Shah (2000)	• “we conceptualized social capital as a multidimensional construct. We distinguished three dimensions: social trust as an interpersonal dimension, life satisfaction as an intrapersonal dimension, and social engagement as a behavioral dimension.” (p.123)
Lin, Cook	• “resources embedded in a social structure which are assessed and mobilized

and Burt (2001)	in purposive actions” (p. 12)
Adler and Kwon (2002)	• “understood roughly as the goodwill that is engendered by the fabric of social relations and that can be mobilized to facilitate action” (p.17)

As might be expected with these varying definitions and suggestions of multiple dimensions, one source of contention within the social capital literature pertains to the multidimensionality of the construct. Another area of debate centred on the consequences that social capital produces. Yet, these arguments are not necessarily distinct. Thus, to understand the dimensions of the construct, the consequences of social capital will be introduced first in Section 2.1.1 followed by a discussion of the dimensions in Section 2.1.2.

2.1.1 Consequences of social capital

One area of contention in social capital research pertains to distinguishing between the sources, consequences and actual constitution of social capital (Newton, 1997; Woolcock, 1998). Indeed, one of the most cited conceptualisations of the construct defined social capital in terms of its functions (Coleman, 1988). Coleman asserted that social capital functioned via obligations and expectations within social relations, via information-flow capability of the social structure, and via norms and related social sanctions among social relations. While Coleman’s work has been integral to the development of social capital theory, it has also been recognised that each of these functions of social capital are more appropriately described as consequences of social capital rather than the definition of the construct (Newton, 1997; Woolcock, 1998) because “defining social capital functionally makes it impossible to distinguish what it is from what it does" (Edwards and Foley, 1997, p.669).

Consistent with Coleman's functions of social capital, social capital has been recognized to provide a variety of other general and specific benefits.

First, social capital offers efficiency. The benefits of social capital can be unique to social capital and thus not achievable in other ways (Putnam 1993). And, although some of social capital's benefits may be achievable in other ways, doing so is only possible at extra cost (Nahapiet and Ghoshal, 1998). Thus, social capital provides efficient access to resources.

A direct, and crucial, benefit of social capital is the flow of information (Coleman 1988; Burt 1992; Nahapiet and Ghoshal 1998; Sandefur and Laumann 1998; Adler and Kwon 2002). Social relations permit the sharing of information among individuals within a social structure. Within social structures are both 'strong' and 'weak' connections or 'ties' and the types of information available through those connections will differ such that weak ties provide information diversity and strong ties provide information depth (Gronovetter, 1973; Sandefur and Laumann, 1998). Information sharing also facilitates access to subsequent benefits by way of conversion of social capital into other forms of capital.

Consequently, that social capital is convertible to other forms of capital is seen as an important benefit (Bourdieu, 1986; Coleman, 1988; Nahapiet and Ghoshal, 1998). In particular, Bourdieu (1986) asserted that social capital could be converted into economic capital in certain circumstances; Coleman (1988) argued that social capital within a family or community could be converted into human capital but also noted that the generators of social capital could capture only a portion of its benefit; and Nahapiet and Ghoshal (1998) argued that social capital permitted the sharing and combination of intellectual capital which ultimately results in the creation of new intellectual capital.

The mutual trust and commitment that exists between two or more individuals independent of a transaction has been coined ‘social solidarity’ (Sandefur and Laumann, 1998, p. 491). Social solidarity has thus been presented as a benefit of social capital (Sandefur and Laumann, 1998; Adler and Kwon, 2002), suggesting that trust and commitment are consequences of social capital that need not be formed via any particular exchange within the relationship. Rather, social solidarity can exist purely by nature of the relationship (i.e. familial, shared culture) but it can also be accumulated as a result of repeated interactions with others.

Numerous other benefits derived from social capital have been discussed in various literatures. For example, in a sociological context, Putnam (2000) asserted that communities with higher levels of social capital benefitted from lower crime rates, better general health, higher levels of educational achievement and greater economic prosperity. In organizational research, social capital has been noted to contribute positively to individuals’ career success (Burt 1992) and to reduce turnover (Krackhardt and Hanson 1993), strengthen supplier relations (Baker 1990) and facilitate entrepreneurship (Chong and Gibbons 1997), among other benefits (Adler and Kwon 2002).

Although the majority of academic attention paid to social capital has been upon its positive externalities, negative aspects and consequences of social capital have also been identified (Portes, 1998; Lin, 2000; Sandefur and Laumann, 1998). Specifically, Portes (1998) identified four negative consequences of social capital:

exclusion of outsiders, excess claims on group members due to norms of reciprocity, restrictions on individual freedoms due to pressures to conform to the group, and 'downward leveling of norms' which results from solidarity and group opposition to mainstream. Lin (2000) further identified unequal access to social capital for women and ethnic minorities given disadvantaged structural positions and networks. Finally, Sandefur and Laumann (1998) stated that "social capital can, in fact, become a liability" (p.493). According to Sandefur and Laumann (1998), the benefit of social solidarity carries with it the liability of stifled innovation and the information benefit associated with social capital carries with it a liability of privacy.

2.1.2 Dimensions of social capital

Despite the cross-disciplinary appeal of social capital as a concept and the important benefits derived from it, an understanding of exactly what is meant by social capital has proved more difficult for scholars to define and a number of scholars have pointed to the likely multidimensionality of the construct. To illustrate the variety of conceptualizations of social capital, Table 2.2 presents the various dimensions of social capital highlighted in the literature by authors asserting a multidimensional representation of the concept[2]. It must be noted that categorizing the dimensions discussed in the literature was not without difficulty, as authors did not employ consistent definitions of dimensions and thus overlap was a common problem. For example, Newton (1997) distinguished three dimensions of social

[2] Although Putnam (1995, 2000) did not present explicit 'multidimensions', his conceptualization is included here because his definitions of social capital suggest trust, commitment, networks and reciprocity are embedded in the construct.

capital (networks, norms and consequences) but discussed trust and reciprocity as crucial norms. On the other hand, norms and trust were discussed distinctly by Nahapiet and Ghoshal (1998) but rather than be considered dimensions of social capital, they were treated as indicators of the relational dimension of social capital.

Table 2.2 Dimensions of Social Capital

	Dimensions of Social Capital										
Author	**Networks**	**Relational**	**Trust**	**Cooperation**	**Commitment**	**Reciprocity**	**Consequences**	**Life satisfaction**	**Civic engagement**	**Integrity**	**Cognitive**
Newton* (1997)	X		X			X	X				
Nahapiet and Ghoshal (1998)	X	X									X
Woolcock (1998)	X	X		X						X	
Paldam (2000)	X		X	X							
Putnam (1995a, 2000)	X		X		X	X					
Scheufele and Shah (2000)			X					X	X		

* Newton (1997) identifies these dimensions from previous literature, but does not defend each dimension. Instead, he offers a critical review.

In spite of these problems, a few notable observations can be drawn from Table 2.2. Similar to Paldam's (2000) five definitions previously introduced, there are three dimensions of social capital commonly ascribed to the construct – networks (Newton, 1997; Nahapiet and Ghoshal, 1998; Woolcock, 1998; Paldam, 2000;

Putnam, 2000), trust (Newton, 1997; Paldam, 2000; Putnam, 2000; Scheufele and Shah, 2000) and cooperation (Woolcock, 1998; Paldam 2000). Other dimensions of social capital identified in the literature that are closely related to cooperation included civic engagement (Scheufele and Shah, 2000) and reciprocity (Putnam 2000). Nahapiet and Ghoshal (1998) specifically identified an unique dimension – the cognitive dimension which was meant to represent shared codes and language and shared narratives among social relations.

The three most prevalent dimensions - cooperation, trust and networks - will be discussed in turn.

Social Capital and Cooperation

Cooperation has been identified as a unique dimension of social capital (Woolcock, 1998; Paldam, 2000) but one can also see how cooperation might be a component of other dimensions identified by authors in Table 2.2.

Specifically, civic engagement (Scheufele and Shah, 2000) requires some level of community cooperation. Similarly, among the general 'consequences' (Newton, 1997) of social capital may be 'cooperation'. Trust and commitment have been explained as a consequence of social capital in the form of social solidarity (Sandefur and Laumann, 1998). Further, reciprocity (Newton, 1997; Putnam, 1995a, 2000) requires cooperation among individuals in social relationship since it "does not entail tit-for-tat calculation in which participants can be sure that a good turn will be repaid quickly and automatically" (p.576). Instead, reciprocity involves uncertainty and vulnerability and requires trust in others to assume that good turns will be paid at some point in the future (Newton, 1997). Inherent in the notion of reciprocity, though, is the idea that individuals will cooperate to return favours.

Just as Coleman's (1988) use of function to define the social capital construct was criticized, a similar argument could be made here. By using explicit 'consequences' (Newton, 1997) to define a dimension of social capital, constructs are being confounded. Rather than being a distinct dimension of social capital, it is more likely that cooperation and the closely related dimensions discussed (civic engagement, commitment, reciprocity, and consequences) are better expressed as distinct consequences of social capital and not used to define social capital. Thus, social capital "forms the foundations of a cooperative and stable social and political order that encourages voluntary collective behavior" (Newton, 1997, p. 576), but cooperation is not social capital.

Furthermore, Paldam (2000) asserted that trust and cooperation were interactive constructs in that trust was primary to cooperation but that cooperation also engendered trust. Similarly, Newton (1997) suggested that trust could facilitate cooperation and also that trust was necessary for reciprocity. Therefore, trust, as a dimension of social capital will be discussed in the next section.

Social Capital and Trust

Expressed simply, trust is "a willingness to rely on an exchange partner in whom one has confidence" (Moorman et al 1993, p.82). By its very nature, it is a collective attribute (Lewis and Weigert 1985) that functions as a basic building block for civil and prosperous society (Blau 1964; Lewis and Weigert 1985) reliant on one's expectations of the behaviour of others (Zucker, 1986; Nooteboom, 2002).

Indeed, Fukuyama (1995, p. 26) declared that "Trust is the expectation that arises within a community of regular, honest, and cooperative behavior, based on commonly shared norms, on the part of other members of that community."

Trust has been argued to be a distinct dimension of social capital by a number of authors (Newton, 1997; Paldam, 2000; Putnam, 2000; Scheufele and Shah, 2000) and, as previously mentioned, seminal social capital works have highlighted the centrality of trust to definitions of social capital (Coleman, 1988; Fukuyama 1995). According to Paldam's (2000) multidimensional perspective of social capital, the one common central area of social capital with the deepest definition deals with trust and Newton (1997) similarly argued that the norms of "trust and reciprocity are crucial aspects of social capital" (p.576). Even authors not specifying trust as a distinct dimension of social capital recognized the necessity of discussing trust in relation to social capital. For example, Nahapiet and Ghoshal's (1998) relational dimension of social capital includes trust as an indicator. However, where Nahapiet and Ghoshal (1998) discussed trust as a 'relational' dimension distinct from other group norms, Newton (1997) included 'norms' of trust and reciprocity together as the overarching dimension of social capital.

Trust, in the context of social capital, can be generalized or special trust (Paldam 2000). Generalized trust, as its name implies, refers to a general trust in people, whereas special trust refers to trust in specific people or particular institutions. Because social structures are comprised of both strong and weak ties (Granovetter, 1973; Sandefur and Laumann, 1998), it follows that individuals would likely have different amounts of trust depending upon the level of connection between parties. According to the notion of special trust, then, individuals do not have a consistent amount of trust in others. As expressed by Putnam (1995b), "I might well trust my neighbours without trusting city hall, or vice versa" (p. 665). It may well be that hierarchical relationships influence trust, particularly among those with whom less direct personal interaction has occurred. Thus, according to Fukuyama (1995, p. 25), "Hierarchies are necessary because not all people within a community can be relied upon to live by tacit ethical rules alone".

Further, because social capital can exist between individual and corporate actors (Coleman 1988), distinctions between types of trust are required for understanding social capital (Dasgupta, 2000), but, "it is not easy to model the link between personal, groups and institutional trust" (Dasgupta, 2000, p. 333). One fundamental distinction that must be made, then, is between organizational and interpersonal trust. Cohen (2001) suggested that organizational trust involved more than reputation and experience which were typical influences upon interpersonal trust. Similar to Fukuyama's (1995) assertion that hierarchies are essential for trust, McCauley and Kuhnert (1992) specified that roles and rules of the organization partly influence organizational trust as well.

The inclusion of trust as a dimension of social capital is a contentious claim, however (Adler and Kwon, 2002). While trust is invariably recognized to be closely related to social capital, some authors have argued that including it as a dimension of social capital leads to problems of confounding constructs (Newton, 1997; Lin, 1999). Woolcock (1998) cited the inherent difficulty in isolating an accurate conceptualization of social capital for reasons of extracting whether constructs such as trust were social capital or sources or benefits of social capital. And, even though Putnam (1995, 2000) used 'trust' and 'trustworthiness' to describe the idea of social capital, he clarified his position in 2001 by stating, "I am in agreement with Michael Woolcock that social trust is not part of the definition of social capital but it is certainly a close consequence, and therefore could easily be thought a proxy" (p. 7).

Social Capital and Networks

Generally, a structural network refers to the relative density of links within the network that facilitate information flow and social support (Wellman and Frank 2001), or more simply, the patterns of connections among relations (Nahapiet and Ghoshal, 1998). The importance of the structural network to social capital was emphasized by Coleman (1988) when he wrote that social capital "is a variety of entities with two things in common: they all consist of some aspect of social structure and they facilitate certain actions of actors" (p. S98). Since Coleman's contribution to social capital literature, the notion of the social structure, or social network, has been consistently identified as a defining characteristic or dimension of social capital (Newton, 1997; Nahapiet and Ghoshal, 1998; Woolcock, 1998; Paldam, 2000; Putnam, 2000).

The literature about social structure discusses that there are different levels of social networks. As Sandefur and Laumeann (1998) clearly indicated, "An individual's potential stock of social capital consists of the collection and pattern of relationships in which she is involved and to which she has access, and further to the location and patterning of her associations in larger space." (p. 484). Thus, there are two important concepts in social structure – network ties and network configuration (Nahapiet and Ghoshal, 1998).

Network ties refer to the relationship of the individual to others. Because of the centrality of the self to the concept, these connections have been referred to as an ‘egocentric’ (Sandefur and Luamann, 1998) perspective of the social network. With this micro orientation (Woolcock, 1998), social capital is characterized by direct relationships with others and by the other people that can be reached as a result of the direct connections (i.e. friends-of-friends) (Sandefur and Laumann, 1998).

Network configuration refers to higher order connections between networks, or a ‘sociocentric’ orientation (Sandefur and Luamann, 1998). At this macro level (Woolcock, 1998), social capital is a by-product of how one’s interactions fit into a larger pattern of interactions within a social system (i.e. community, culture, nation).

Adler and Kwon (2002), distinguished three types of social structure – market relations, hierarchical relations and social relations –explained by the types of exchange involved in the connection. Market relations involve the symmetrical exchange of goods and services for money with specific and explicit terms of exchange. Hierarchical relations are asymmetrical and require obedience to authority in exchange for material or spiritual security. Hierarchical relations are characterized by explicit terms (i.e. contract) that are diffuse (exhaustively specific terms that are not agreed to up-front). Social relations involve symmetrical exchanges of favours and gifts, but the terms of the exchange are diffuse and based upon tacit understandings of reciprocity among connections. According to the authors, it is social relations that “constitutes the dimension of social structure underlying social capital” (Adler and Kwon, 2002, p.18) but also acknowledge that “any concrete relationship is likely to involve a mix of all three types” (p.19).

Among social relations, an important structural distinction has been made based upon the degree of connectedness between relationship partners or ‘ties’. Thus, it has been suggested that interpersonal connections can either be ‘strong ties’ or ‘weak ties’ (Granovetter, 1973). Although Granovetter (1973) did not discuss social capital directly, his work has been influential in explaining the nature of networks via the distinctions he articulated between these types of interpersonal ties. Granovetter (1973) argued that the strength of interpersonal connections, or ties, resulted from the combination of “the amount of time, the emotional intensity, the intimacy (mutual confiding) and the reciprocal services which characterize the tie (p.1361).

Granovetter’s contributions have been foundational in subsequent distinctions between two different kinds of social capital – bridging social capital and bonding social capital (Putnam, 2000). The crucial difference between these two types of social capital is the type of socializing that takes place within the relationship (Coffé and Geys, 2007). Bonding associations tend to exist within tightly knit groups that typically include family and close friends (Putnam 2000) or people with homogeneous backgrounds (Coffé and Geys, 2007). Bonding social capital involves trust and reciprocity and provides emotional support (Putnam, 2000) and results in reinforcement of shared codes, narratives and language, or cognitive social capital (Nahapiet and Ghoshal, 1998). In contrast, bridging social capital typically provides information, but little emotional support, among individuals whom are loosely connected, or ‘weak ties’ (Granovetter, 1973; Granovetter 1982; Putnam 2000). Bridging associations connect diverse individuals and reduce the redundancy of information shared (Putnam, 2000) and thus may create opportunities for conversion of social capital to other types of capital including financial, human (Putnam, 2000) and intellectual (Nahapiet and Ghoshal, 1998). Accordingly, Putnam (2000) proclaimed that bonding social capital was good for "getting by" and bridging social capital was necessary for "getting ahead" (p.23).

Despite the lack of clarity and agreement on social capital presented thus far, it is clear that social capital is a widely accepted construct with value in social science research. From the various conecptualisations of the social capital construct, it has been made evident that cooperation among individuals was a positive consequence of social relationships. It was also shown that, although not truly social capital, trust was a closely linked construct that makes a good proxy for social capital. Finally, the literature suggested with consistency that social capital was most appropriately described in terms of social relationships and that both network ties and network structure were important components of social capital.

There are a number of social networks within which any one individual interacts and may acquire social capital. Though foundational social capital research had been conducted among traditional social networks including families, work and community groups, interest has recently been directed toward social capital in online environments (Blanchard and Horan, 1998; Wellman et al, 2001; Wasko and Faraj, 2005; Best and Kreuger, 2006; Chiu, Hsu and Wang, 2006). In these environments social capital outcomes were found to be complementary to those realised in physically based communities (Blanchard and Horan, 1998), the essential knowledge sharing component of social capital was evident in Internet-based communities (Wasko and Faraj, 2005; Chiu, Hsu and Wang, 2006), the Internet supplemented communications typically occurring through more traditional mediums among social network connections separated by a distance (Wellman et al, 2001) and the Internet facilitated social capital generation through expanded network connections (Best and Kreuger, 2006). In light of these insights it stands to reason that social capital likely exists within a special type of Internet Based community – the online social network. Further, given the commonly held understanding that social capital is ultimately a function of one's social structure and ties (Newton, 1997; Nahapiet and Ghoshal, 1998; Sandefur and Laumann, 1998; Woolcock, 1998; Paldam, 2000; Putnam, 2000), and that online social networks (OSNs) are comprised of little more than social connections facilitated by technological platforms, social capital theory appears especially appropriate in the context of OSNs. Consequently, the remainder of this chapter will emphasize online social networks and discuss connections of social capital theory in these environments.

2.2 Online Social Networks

The term 'social network' is a theoretical concept frequently used in social and behavioural sciences to describe a social structure comprised of a set of actors and their dyadic ties. Specifically, it has been defined as a "set of people (or organizations or other social entities) connected by a set of social relationships, such as friendship, co-working or information exchange" (Garton, Haythornwaite and Wellman 1997, p. 3). Although the concept was foreshadowed in writings dating back to the ancient Greeks, John A. Barnes is credited with having been the first to utilize the term in a scientific sense in a 1954 anthropological study (Barnes 1954; Wikipedia(a)). As "computer networks are inherently social networks" and computer-mediated communication has become common practice in the lives of individuals (Wellman, 2001, p. 2031), the term ‘social network’ has been popularized to refer to “a dedicated website or other application which enables users to communicate with each other by posting information, comments, messages, images, etc.” (Oxforddictionaries.com, 2012). However, to distinguish these computer-mediated social networks from the broader concept that includes offline interactions among individuals, academic researchers investigating the very specific type of social network which occurs in online communities have referred to these environments as ‘social networking sites’ (SNS) or ‘online social networks’ (OSNs).

2.2.1 Definition of online social networks

In essence, an OSN is a user-generated online community comprised of “the *people* who come together for a particular *purpose*, and who are guided by *policies* (including norms and rules) and supported by *software*” (Preece and Maloney-Krichmar, 2006). These fluid and flexible communities develop, “when enough people carry on computer-mediated nonprivate discussions long enough, with sufficient human feeling, to develop what are considered ‘social relationships’ with other online participants” (Brown, Broderick and Lee, 2007, p.3; Rheingold, 1993).

The widely accepted scientific definition of an online social network is “web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system” (Boyd and Ellison 2007, p.211). The individuals with whom one connects within online social networks may be referred to as ‘friends’ but different nomenclature exists depending upon the website providing the infrastructure. Other names for one’s connections include, but are not limited to, ‘follower’, ‘subscriber’, ‘professional’ and ‘relative’ (Beye et al 2010). No matter the terminology used, these connections include offline friends with whom one regularly interacts, friends from the past, colleagues, current and former classmates, acquaintances and new affiliations created through online interactions. Although the connections articulated in these environments frequently include those with whom one has regular offline contact, the networked public created through online social networks has been argued to be distinguishable from typical face-to-face public life by four properties. Specifically, Boyd (2007) suggested that because information shared among connections in online social networks is persistent, searchable, replicable, and can be viewed by invisible audiences the nature of the networked public and social dynamics become fundamentally altered.

As Boyd’s definition further suggests, construction of a personal profile and display of an identified list of connections are requisite features of OSNs. Clearly then, disclosure of certain amounts of personal information is required to become a member of an OSN. The amount of information disclosed in the personal profile is normally left to the discretion of the user, but the user’s name (or pseudonym), birthday (but not necessarily birth year), and email address are typically required pieces of personally identifiable information. The discretionary elements in a personal profile might include information pertaining to education, employment, activities, interests, hobbies, relationship status, sexual orientation, birth year, or favourite quotes. Depending upon the website’s functionality, other data including private messages, public comments, photos, videos, tags, preferences, groups and behavioural data may be exchanged as well (Boyd and Ellison 2007; Beye et al 2010).

Given the potential volume of information exchange and the apparent degree to which people share in these environments has prompted Andrew Keen (2012) to suggest online social networks have become, a "permanent self-exhibition zone of our new digital age". The importance of OSNs to daily life is emphasized further by Keen in the following comment:

> "This place is built on a network of increasingly intelligent and mobile electronic products that connect everyone on the planet through services such as Facebook, Twitter, Google+ and LinkedIn. Rather than a virtual or second life, social media is becoming life itself -- the central and increasingly transparent stage of human existence, what Silicon Valley VCs now call an "internet of people".

2.2.2 Types of OSNs

There are many types of OSNs, yet there are few scientific classifications of these sites (Beye et al 2010). The available classifications tend to be found on pseudo-scientific blogs or within online marketing resources. These classification systems typically group sites based upon topical coverage, breadth of the user base, openness of the network, or type of networking that occurs (Beye et al, 2010).

Only one classification of OSNs derived through empirical analysis was uncovered in the course of this literature review. In a study conducted in Tokyo, Toriumi et al (2011) used a cluster analysis of data from 615 OSNs to conclude the existence of four different types of OSNs based upon users' communication patterns on the sites. Specifically, these were:

1) Partial friend network wherein members communicate only with a small group of friends

2) Parity friend network wherein members communicate with their network friends and *few* communicate outside their friend network

3) Inclusive friend network wherein members communicate with their network friends and *many* communicate outside their friend network

4) Independent friend network wherein members communicate independently of their friend network

From this classification system one can see parallels to Granovetter's (1973) concepts of 'strong ties' and 'weak ties', but use of Toriumi et al's (2011) classification for a practical understanding of the types of OSNs would be difficult. This classification relies on understanding the communication patterns of individuals within OSNs generally, but whether the observed communication behaviour was specific to particular OSNs was not investigated nor was the role individual characteristics might play in one's affinity for particular types of network communication. This means that it is possible to envision that among one online social networking site's membership, all four types of Toriumi's networks may exist thus making practical discussion of OSNs via this classification impossible.

Another classification system appearing in academic literature grouped OSNs according to five generic business models (Kasavana et al 2010[3]). According to the authors, the types of OSNs are as follows:

1) General – an OSN to meet, socialize and share content and interests with friends such as Facebook, Orkut and MySpace

2) Practice – an OSN that facilitates connections between professionals and practitioners such as LinkedIn and Plaxo

3) Interest – an OSN emphasising connections between individuals holding common interests in a subject area such as politics (E-democracy.org), health or finance.

4) Affinity – an OSN focusing on self-identification with a demographic or geographic category such as women (iVillage)

5) Sponsored – an OSN created by commercial, government or nonprofit organizations such as Nike.

In essence, Kasavana et al's classification system grouped OSNs by the purpose of connections or the purpose of use of the site. While logical, this type of classification appears to require further refinement as it is difficult to clearly distinguish between general, affinity and interest types of OSNs. For example, one may join a certain political OSN because they self-identify with a particular political ideology thus obscuring the delineation between an interest and affinity OSN per the descriptions above. Similarly, if one's purpose for joining an OSN such as iVillage

[3] While Kasavana et al (2010) cite Lenard (2004) as the source of this classification, the Lenard article indicated by Kasavana et al bears no mention of such a classification. As such, credit for this classification system is attributed to the authors in which it appeared but one must recognize Kasavana et al are unlikely the originators.

was to share content with new contacts or ‘friends’, the distinction between general and affinity OSNs becomes less clear.

A more refined OSN classification system broadly based upon purpose of use was formulated by Beye et al (2010) as a result of similar issues of taxonomy overlap identified among pseudo-scientific blog classifications. These authors proposed identifying online social networks as either primarily ‘connection’ sites or ‘content’ sites with subcategories of each type. Connection sites “focus more on the connections users have and exploit this mainly by (re-)connecting users and providing a social contact book” (Beye et al, 2010, p.4). Subcategories of connection sites include *dating* sites such as Match.com, *business* sites such as LinkedIn, sites *enforcing real-life relationships* such as Classmates.com, and *socializing* sites such as Facebook, Orkut and MySpace. In contrast, content sites focus on the content provided or linked to by users. Subcategories of content sites include: *content sharing* sites that rely on sharing user-generated content such as Flickr and Pinterest; *content recommendation* sites that focus on recommending already existing content rather than user-generation such as WeRead.com; *entertainment* sites that focus on gaming such as Xbox and Playfire; *advice sharing* sites where individuals with some expertise on a topic offer advice such as BabyCenter; *hobby* sites that, while similar to advice sharing sites, are distinguishable based on a more homogenous membership, and *“news” sharing* sites that emphasise sharing world news and gossip such as Twitter and Blogster.

2.2.3 OSN Users

Given the many types of OSNs and the numerous purposes of use identified in the previous section, one might assume that there is something for everyone. Indeed, with 1.43 billion people worldwide (approximately 20% of the global population) predicted to use a social networking site in 2012 and 25% participation forecast by 2014, claims of OSN ubiquity are understandable (eMarketer, 2012). Among Internet users, OSN penetration is even higher, with 63% of connected individuals worldwide expected to visit a social network site at least once per month in 2012.

While it is difficult to conclude usage statistics for online social networks with complete accuracy due to fluidity in memberships, the release of membership data from private entities and slight variability in user reported participation rates compiled from various research organizations, many reports place Canada, the United States and the United Kingdom among the most 'socially networked' countries in the world. Based solely upon the total number of OSN members, the top social networking markets in 2012 were the United States, India, Brazil, China and Russia (eMarketer, 2012). However, based upon the proportion of Internet users using OSNs per country in 2008, Canada (53%), the United Kingdom (39%), and United States (34%), and Japan (32%) represented the markets wherein OSN penetration was highest (Ofcom 2008). In 2011, Canada's social networking penetration had grown to 47% of the total population (60% of Internet users) and represented the country with the highest social networking penetration per capita followed closely by the United States (Oliveira, 2012). In the same year, UK penetration had increased such that 59% of online adults had a profile on an OSN (Ofcom, 2012).

While these statistics clearly indicate that online social networks are used by a substantial proportion of the population in the countries identified above, participation rates hovering close to 50% of the total population do not technically establish a case for true ubiquity. One reason offered for less than maximum participation in OSNs may be a ‘participation divide’ that can result from socioeconomic barriers to Internet access. Due to resource constraints, certain socioeconomic demographics may still not have access to the Internet at home and thus OSN participation is beyond their reach because OSN usage may be banned in schools or at work (Hargittai, 2008; Boyd, 2007). Others conscientiously abstain from OSN participation as a result of technological inexperience, safety concerns and related parental bans, or pure intellectual rejection of OSNs (Boyd, 2007; Ofcom, 2008).

Despite the apparent participation divide created through resource constraints or conscientious objection, age is no longer a barrier to OSN participation. Though OSN participation was originally strongest among youth and many OSN sites are still dominated by this demographic, older adults are using OSNs worldwide as well. In Canada, 86% of online 18-24 year olds participate in OSNs, but a majority of online Canadians in the 35-54 year range are also OSN members and the percentage of 55+ year old online Canadians participating in these environments has grown to 43% (Ipsos, 2011). In the United States, 60% of online 18-29 year olds used social networking sites in 2010 compared with 39% of those aged 30-49, 20% of those aged 50-64 and 13% of those 65 and older (Madden, 2010). In Great Britain, 91% of 16-

24 year old Internet users participated in OSNs in 2011 but almost one fifth of Internet users aged 65 and older did so as well (Office for National Statistics, 2011).

Interestingly, a slight gender divide has been noted in participation rates in OSNs. Although men have been noted to be more savvy networkers than women on professional OSNs like LinkedIn (Rapleaf, 2008; Nicholson, 2011), many market research polls reveal that OSN participation is higher among women. For example, a commissioned Harris Interactive study undertaken in May 2011 across the United States revealed that women were significantly more likely than men to use OSNs to communicate with work colleagues (34% v. 22%), family (60% v. 42%) and friends (68% v. 54%) (PRWeb, 2011). Similar statistics citing heavier OSN participation among women have been reported in both Great Britain and Canada as well. Specifically, in Great Britain, 60% of female internet users used OSNs compared with 54% of their male counterparts (Office for National Statistics, 2011) and female online Canadians were more likely than men to be frequent users of OSNs, having visited an OSN site at least daily (37% compared with 24%) (Ipsos, 2011).

2.2.4 Popular OSNs

Although there are numerous OSN websites to cater to the many users identified in the previous section, some are more popular than others. As of May 2012 there were 13 social networking websites with memberships in excess of 100 million (Wikipedia, 2012b), though a Real Time Report for February 2012 indicated there were only seven sites reaching this criteria and only five of the sites identified in the Real Time Report overlapped with Wikipedia's list. Table 2.3 provides an overview of the membership statistics for the top global OSNs published in both these sources along with the most recent publicly available membership data compiled from various sources by this author. In order to permit some comparison by type of OSN, Beye et al's (2010) classification has been attempted for each of these popular sites as well.

As Table 2.3 illustrated, Facebook was clearly the dominant global OSN[4]. Developed in 2004 by then university student Mark Zuckerburg, Facebook has grown from serving the Harvard campus community to become the dominant online social network provider in three of the five top social networking markets worldwide - US, India and Brazil with 141 million, 68.1 million and 45.4 million users respectively (eMarketer, 2012). Approximately half of the population of the United States is a Facebook member. In Canada, Facebook is not only the most dominant social network site, the OSN is the most used website in the country, capturing the highest market share of visits as recently as May 2012 (Experian Hitwise, 2012). Among social networking sites, it received a 64% share of visits from Canadians for the week ending May 5, 2012 compared with number two ranked YouTube (21% share of visits) and number three ranked Twitter (1% share of visits). According to

[4] Reporting precise numbers for Facebook membership can be challenging as it changes daily and there are minor discrepancies in the membership numbers reported in published sources. At the time of writing, Facebook reportedly had 837.2 million users in March 2012, a 27% increase from 2011 (eMarketer 2012). Yet, Facebook disclosed its membership at 845 million members when it filed its $5 billion IPO with the U.S. Security Exchange Commission in February, 2012 (PCMag.com). Figures reported in April 2012 indicated that the number of monthly active users (MAUs) on the site had surpassed 900 million, an increase of 32% from the same period one year prior and daily active users had increased by 41% in the same time period (PCMag.com).

one report, 59% of Internet users in Canada are Facebook members and among OSN users, almost all (95%) retain Facebook memberships (Oliveira, 2012).

Table 2.3 Social Networking Site Membership as of May 2012

Social Networking Website	**Classification (based upon Beye et al 2010)**	**Home Country**	**Number of Registered Members (Wikipedia 2012b)**	**Number of Registered Members (McNaughton 2012)**	**Number of Registered Members (updated by author[5])**
Facebook	Connection - socializing	US	901,000,000	845,000,000+	
Qzone	Connection - socializing	China	480,000,000	500,000,000	
Weibo	Content – news sharing	China	n/a	250,000,000+	
Twitter	Content – news sharing	US	300,000,000	200,000,000	
Habbo	Connection - socializing	Finland	200,000,000	n/a	230,000,000 (Habbo.com)
Google +	Connection - various	US	170,000,000	90,000,000	
Renren	Connection - socializing	China	160,000,000	170,000,000	
Badoo	Connection - dating	UK	133,000,000	n/a	153,000,000 (Badoo.com)
LinkedIn	Connection - business	US	120,000,000	150,000,000	161,000,000 (LinkedIn.com)
Bebo	Connection - socializing	US	117,000,000	n/a	
Groupon	n/a	US	n/a	115,000,000	
Vkontakte (VK)	Connection - socializing	Russia[6]	111,578,500	n/a	
Tagged	Connection - socializing	US	100,000,000	n/a	330,000,000 (Raice 2011; Tseng 2011)
Orkut	Connection - socializing	US	100,000,000	n/a	29,000,000 (Geromel, 2011)
Myspace	Connection - socializing	US	100,000,000	n/a	

The next two OSNs with the highest membership numbers, Qzone (500 million) and Weibo (250 million), cater to the Chinese market. Qzone can be

[5] Only those statistics that were not current were updated by this author on May 22, 2012.
[6] VK was founded in Russia but its holding company is located in the British Virgin Islands.

considered a connection site primarily used by mainland Chinese for socializing whereas Weibo is a microblogging site owned by Sina Corp. that is considered comparable to Twitter. Thus, according to Beye et al's (2010) classification, Weibo would be a considered a content site for the purposes of news sharing.

Leveraging the worldwide popularity of Facebook, imitative sites including Renren and Vkontakte (Vk) have been developed for international markets. Renren, "the Facebook of China" (Chao, 2011) provides the same functionality as Facebook to users in Chinese language. Vkontakte, another 'Facebook clone' (Ostrow, 2007) developed for the Russian market, goes as far as duplicating the colour scheme, layout and graphics of Facebook circa 2006, rendering the difference between the two almost impossible to distinguish.

In addition to Facebook, Twitter, LinkedIn and Google+ are the popular OSNs in Canada the United States and United Kingdom and therefore deserve special mention.

Twitter, a microblogging OSN that allows members to share news in 140 characters or less has the most members in the United States, Brazil, Japan and the United Kingdom (Arthur, 2012). Approximately 13% of the American adult Internet user population has a Twitter account (Smith, 2011). With UK Twitter members totaling 10 million, the UK represented the fourth largest national membership on the globe (Arthur, 2012). And, Canadians continue to register high per capita usage of this OSN. According to one calculation, uptake of Twitter is similar in Canada with approximately 14% of the population (20% of Internet users) using the service (Gauthier, 2011). Two unique characteristics about Twitter include its tendency to be accessed by mobile devices (Arthur, 2012; Smith, 2011) and its preference among non-white Internet users in the United States with 25% of African Americans and 19% of Hispanic Internet users holding a Twitter account compared with 9% of white respondents (Smith, 2011).

LinkedIn is the world's largest OSN dedicated to fostering professional connections. The site provides service available in seventeen languages to approximately 161 million members worldwide. Membership is heavily American (39%) yet memberships are held globally. Five percent of members reside in the UK and 3% reside in Canada (LinkedIn, 2012). Its membership tends to be slightly skewed toward males. In Great Britain, 16% of male Internet users participated on this site compared with only 9% of females (Office for National Statistics, 2011).

Google+, did not meet the 100 million member threshold with the most recently published official data as of January 2012. However, its recent gains in popularity in conjunction with projections the site will represent genuine competition to Facebook by reaching 400 million members by the end of 2012 (Thornhill, 2011) make it noteworthy. Rather than becoming a clone of Facebook, Google+ has added user controls that meet an unmet demand among Facebook users. In particular, within Google+ one may create 'circles of friends' such that the user may classify groups of friends so that when they choose to disseminate information in the OSN they retain greater control over which of their friends see the posts. For example, in Google+ one may designate a certain group of people 'family' another 'colleagues' and another 'friends'. When choosing to share information, such as pictures of an evening out with friends, the user would likely select to share that information with their Google+ friends but not provide access to their 'colleagues' nor possibly their ‘family’. Other improved user controls offered by Google+ include increased control over personal data ownership and permission based photo tagging (Sullivan, 2011).

Google+ appears intended to be a connection site, but the ability to designate circles of friends allows the varied purposes for those connections to exist on one site, thus making this new site difficult to classify with Beye et al’s (2010) structure. It is easy to see that one may use the site to socialize with ‘friends’, network and share work-related information with ‘colleagues’ or even use the site for dating purposes by designating a circle of friends accordingly. Coupled with Google’s many other services including their powerful search engine, the Google+ user is able to more easily share content and news with his or her respective circles of friends, thus blurring the distinction between Beye et al’s major ‘connection’ and ‘content’ classifications of OSNs.

Groupon is yet another OSN that is difficult to classify using the structure proposed by Beye et al (2010). Groupon works by bringing together disparate individual buyers into groups so that they might make volume purchases from sellers thereby receiving price discounts. If a large enough group commits to purchasing a posted deal, the discount price is paid for the product or service. If there is insufficient interest in a deal the discount rate is not offered but the interested parties are not obligated to purchase the product or service. While purchasing a particular deal through one’s Groupon membership might be considered a social act in that numerous others are required to purchase the same deal, it is not required that other the purchasers on the deal be connected in any way. Groupon members are encouraged to leverage their connections within other OSN sites by posting Groupon deals on Facebook.

The discussion thus far indicates that OSNs serve basically as tools for connection and content sharing. And, as Table 2.3 also illustrated, the most popular OSNs globally were generally those classified as connection sites intended for socializing. Yet, that so many individuals around the globe have so readily adopted OSNs, a systematic understanding of users' motives for participating in these environments was required. Consequently, the motivations identified through scientific inquiry are discussed in Section 2.3 and 2.3.1.

2.3 Motivations for OSN participation

People choose to participate in OSNs to connect with others and to share various types of content among those connections but the underlying motivations for desiring those connections can be varied. In a 2008 qualitative study of UK adults aged 16 and older, Ofcom identified five different types of OSN user based upon one's purpose for membership. Specifically, there were 'alpha-socializers' (those that participate for short bursts of time to flirt, make new connections and for entertainment purposes), 'attention seekers' (those that sought attention either through posting comments, photos or customized profile elements), 'followers' (those that join to keep up with their peers), 'faithfuls' (those that join in search of former friends and classmates) and 'functionals' (those that participate for a specific purpose) (Ofcom, 2008). Among all of these types of users, Ofcom had found that 'followers' and 'faithfuls' represented the majority of OSN users.

In addition to surveys conducted by public sector organisation such as Ofcom, there has recently been significant academic inquiry into OSN participation motives. An overview of that research is provided in Table 2.4.

A variety of research approaches ranging from qualitative (Boyd 2007; Livingstone, 2008; Palmer and Koenig-Lewis, 2009; Dunne, Lawlor and Rowley, 2010) to mixed methods (Hart, 2008; Joinson, 2008; Lee, Im and Taylor, 2008; Pfeil, Arjan and Zaphris, 2009) to purely quantitative approaches were used to examine OSN motivations within the literature. Examination of sample demographics indicated analyses have been more strongly centred upon younger, university-educated and slightly more female populations which are consistent with early adopter OSN population demographic characteristics. A majority of studies were set in the United States, just as many of the most popular OSNs are headquartered there, but perspectives from the UK, Ireland, Hong Kong, Korea, Australia and Ireland were also captured. While most studies appearing in Table 2.4 concentrated upon Facebook as the OSN of interest, other OSNs with specific regional popularity were used as reference on occasion (i.e. Dunne, Lawlor and Rowley (2010) investigated Ireland's popular OSN Bebo). In five instances responses were not constrained to any one OSN (Dholakia et al, 2004; Lee et al, 2008; Livingstone, 2008; Subrahmanyam et al, 2008; Young, 2009).

Table 2.4 Overview of OSN Motivations Literature

Study	OSN	Sample Geography	Sample Size (N=)	Sample Gender (% Female)	Sample Age (Avg in yrs)	Students (% Sample)	Research Method (analytic technique)
Dholakia, Bagozzi and Pearo (2004)	Various	Global	545	41.8%	33.1	n/a	Quantitative (CFA and SEM)
Acquisti and Gross	Facebook	US	294	50%	n/a	89.46	Quantitative (descriptive)
Lampe, Ellison and Steinfield (2006)	Facebook	US	1,440; 1,085	n/a	n/a	100	Quantitative (descriptive)
Boyd (2007)	MySpace	US	n/a	n/a	Under 18	n/a	Qualitative (ethnographic)
Ellison, Steinfield and Lampe (2007)	Facebook	US	286	66%	20.1	100	Quantitative (regression)
Hart et al (2008)	Facebook	UK	26	61.5%	n/a	85	Mixed Methods
Joinson (2008)	Facebook	UK	137; 241	64.2%; 66.8%	26.3; 25.97	n/a	Qualitative; Quantitative (EFA)
Lee, Im and Taylor (2008)	Bloggers	Korea	259	42.4%	n/a	94.6	Mixed Methods (Depth interviews; EFA, CFA & SEM)
Livingstone (2008)	Various	UK	16	50%	Under 16	n/a	Qualitative (in person open ended interviews)
Steinfield, Ellison and Lampe (2008)	Facebook	US	286; 481	66%; 67%	20.1; 20.6	100	Quantitative (regression & correlation)
Subrahmanyam et al (2008)	Various	US	110	50%	21.5	100	Quantitative (Descriptive & 2x2x2 contingency tables)
Young (2009)	Various	Australia	752	75.7%	n/a	47.6	Quantitative (descriptive)
Cheung and Lee (2009)	Hong Kong Education City Teachers Channel	Hong Kong	315	48%	n/a	n/a	Quantitative (PLS)
Palmer and Koenig-Lewis (2009)	n/a	n/a	n/a	n/a	n/a	n/a	Qualitative (lit review/ commentary)

Pfeil, Arjan and Zaphiris (2009)	MySpace	UK	100 ; 140	50%	50% teen; 50% 60+	n/a	Qualitative (Content analysis)
Valenzuela, Park and Kee (2009)	Facebook	US	2,603	66.3%	20.88	100	Quantitative (hierarchical multivariate ordinary least squares (OLS) regression)
Cheung and Lee (2010)	Facebook	Hong Kong	389	46%	n/a	100	Quantitative
Dunne, Lawlor and Rowley (2010)	Bebo	Ireland	24	100%	Under 14	100	Qualitative (focus groups; semi-structured interviews)
Hoadley et al (2010)	Facebook	US	172	52%	n/a	100	Quantitative
Cheung, Chiu and Lee (2011)	Facebook	Hong Kong	182	n/a	n/a	100	Quantitative

2.3.1 Social Capital as Motive for OSN Participation

The literature that explored users' motivations for OSN participation (Table 2.4) did so using a variety of theoretical frameworks. Many of the studies were exploratory in nature and thus relied upon reporting descriptive statistics for numerous popularly cited motivations for OSN use. Those that were grounded in theoretical concepts utilized either a uses and gratifications theoretical framework or social capital to understand OSN participation. One article, which did not collect primary research, attempted to conceptualize motivations for OSN participation from a consumer perspective.

Though various theories guided the studies, different OSNs were investigated and samples were drawn from a variety of geographic locations, similarities among conclusions about individuals' OSN motivations were observed and demonstrated obvious connections with concepts of social capital previously introduced. To structure this discussion, findings presented in the literature will be considered according to the theoretical framework employed. Accordingly, the following discussion will begin with the less grounded results accumulated through exploratory research approaches. Findings established within studies grounded in uses and gratifications literature follows. Subsequently, results derived from social capital embedded studies are presented. Finally, the results from the various research frameworks are summarised according to social capital concepts to clearly illustrate the connection.

OSN Motivations Revealed through Exploratory Research Approaches

Within the literature reviewed, eight of twenty studies used exploratory research approaches to determine why individuals participated in OSNs. From these studies, six common themes emerged as reasons for individuals to participate in OSNs including relationship maintenance, self-presentation or identification, entertainment, information, popularity, and social discovery. Table 2.5 identifies the common themes.

Relationship Maintenance

'Relationship maintenance' was commonly identified as an important motivation for OSN participation (Acquisti and Gross 2006; Boyd 2007; Lee et al 2008; Livingstone 2008; Subrahmanyam et al 2008; Young 2009; Hoadley et al 2010). Though not explicitly described as such in all reviewed studies, 'keeping in

Table 2.5 Motivational themes for OSN use within Exploratory Research

Motivational Theme	**Studies**
Relationship Maintenance	Acquisti and Gross (2006); Boyd (2007); Lee et al (2008); Livingstone (2008); Subrahmanyam et al (2008); Young (2009); Hoadley et al (2010)
Self-presentation	Acquisti and Gross(2006); Boyd (2007); Lee et al (2008); Livingstone (2008); Hoadley et al (2010)
Entertainment	Boyd (2007); Hart et al (2008); Lee et al (2008); Young (2009)
Information	Acquisti and Gross(2006); Hart et al (2008); Lee et al (2008); Young (2009); Hoadley et al (2010)
Popularity	Acquisti and Gross(2006); Lee et al (2008); Subrahmanyam et al (2008)
Social discovery	Acquisti and Gross(2006); Hoadley et al (2010)

touch', 'convenience of making contact', 'socializing', and 'intimacy' were all thought to represent elements of relationship maintenance and therefore included in this classification. As connections between individuals in OSNs are frequently between individuals who are known to each other offline (Boyd and Ellison, 2008; Haythornthwaite, 2005), relationship maintenance purposes of OSN use were considered distinct from those of making new friends.

Consistent with a recent public opinion poll that identified an overwhelming majority of American teen (91%) and adult (89%) internet users use social networking sites to stay in touch with friends (Lenhart, 2009), a number of the reviewed studies explicitly identified 'keeping in touch' among the most important reasons for OSN use among respondents (Subrahmanyam et al, 2008; Young, 2009; Hoadley et al, 2010). As previously noted, OSN use is particularly high among younger adults and it has been suggested that social network sites are important to young adults when they are moving away from home and into universities (Steinfield, Ellison and Lampe, 2008). That relationship maintenance was identified as an important motivation of OSN use was not unexpected given that five of the seven samples drawing such a conclusion were comprised of a majority of university students (Acquisti and Gross, 2006; Lee et al, 2008; Subrahmanyam et al, 2008; Young, 2009; Hoadley et al, 2010).

Self-presentation

Boyd (2007) noted that identity construction and identity presentation are critical reasons for OSN participation suggesting that the profiles created on OSN sites allow one to 'write themselves into being' and further communicate a sense of self through the friendship connections displayed on the site because 'you are who you know'. These findings are consistent with Zhao et al (2008) who concluded that college students' Facebook identities were different from those presented to their offline connections and different still from those created in anonymous environments. These authors suggested that because OSNs such as Facebook enable creation of a disembodied identity anchored by one's offline self, people tend to show rather than tell others about themselves and project highly desirable sociable identities - their 'hoped for possible selves' – rather than their 'true selves' or 'real selves'. Similarly, Lee et al (2008) found that 'self-presentation and 'showing off' were popular motivations for OSN participation; and Hoadley et al (2010) concluded that 'showing information about myself' was quite important to the sample, reporting a mean score of 3.20 (on a 5 point Likert scale) for this variable. Interestingly, Acquisti and Gross (2006) found that respondents felt self-presentation was a motive for OSN participation among their peers, but did not identify it as a critical reason for their own participation, perhaps as a result of a social desirability bias in responses.

Though support was shown for self-presentation and identity construction as key motivations for OSN participation, the mechanism by which that presentation occurs may vary by age. For example, Livingstone's (2008) qualitative investigation of teens in the UK revealed that 'identity' was a vital motivation for OSN participation but also noted a distinction between the profiles constructed of younger versus older adolescents. While younger adolescents tended to present visually elaborate constructions of themselves, older adolescents adopted aesthetically plain profile appearances instead focusing on highlighting their social connections (Livingstone, 2008). Likewise, Strano (2008) revealed differences between age and gender in self-presentation via Facebook profile pictures.

Popularity

Popularity is a motivational theme that is closely linked with identity construction and information disclosure (Christofides et al, 2009). Just as Boyd (2007) suggested that 'you are who your friends are', Christofides et al (2009) argued that identities in Facebook are co-constructed. Because information disclosure increased perceived popularity and perceived popularity ultimately leads to identity construction, Christofides et al (2009) concluded that one's need for popularity significantly predicted information disclosure on Facebook. Further, because Facebook removes communication barriers between people who are loosely connected, the OSN proved helpful in facilitating social relationships for individuals with lower self-esteem (Steinfield, Ellison and Lampe's 2008).

However, while popularity as a motivation for OSN participation was frequently discussed in the literature reviewed, its conclusive link was not clearly demonstrated. A confirmatory factor analysis of responses in Lee et al's (2008) research indicated that 'keeping up with trends' was one important factor in OSN participation and Subrahmanyam et al (2008) revealed that 61% of respondents participated in OSNs because their friends had accounts. While these results do not indicate one's specific need for popularity as a motivation for participating in OSNs, they do suggest a social pressure motivation and were used to infer a popularity theme within the reviewed literature. Of course, a social desirability bias might affect the inclination of respondents to report popularity motivations as well. Respondents in Acquisti and Gross's (2006) research reported popularity was likely a motive for their peers' participation in OSNs, but not their own. Similarly, only 9% of respondents in a sample of Australian Facebook users expressed popularity as important for OSN participation (Young 2009) and although increasing popularity was presented as a response option in Hoadley et al's (2010) study, the mean score for ratings of this measure were low for both one's own reasons for Facebook use and the perceived reasons of others.

Entertainment

Regardless of analytical method employed, entertainment was yet another motivational theme concluded in half of the exploratory studies reviewed (Boyd, 2007; Hart et al, 2008; Lee et al, 2008; Young, 2009). Boyd's ethnographic study (2007) of adolescents revealed entertainment was a critical reason for participating in OSNs. Young's (2009) descriptive statistics revealed entertainment was a popularly cited reason (61% respondents) for Australian participation in OSNs as well. Hart et al (2008) reported that among its UK sample, some of the most sought experiences for using Facebook included enjoyment, fun and excitement. Finally, Lee et al (2008) conclusively showed that entertainment was clearly a distinct motivational factor for OSN participation via confirmatory factor analysis.

Information

Information sharing was noted to be another motivational theme for OSN participation in a number of studies reviewed (Acquisti and Gross, 2006; Hart et al, 2008; Lee et al, 2008; Young, 2009; Hoadley et al, 2010). Communication with others either via one-way channels of information posting or receiving and more traditional two-way channels between parties were commonly cited reasons for participating in OSNs. In terms of one-way channels, Hoadley et al (2010) revealed that publicizing news was important to their respondents whereas the curiosity of learning about classmates (Acquisti and Gross, 2006), browsing others' pictures and profiles (Hart et al, 2008) and simply 'follow[ing] what is happening in the lives of others' (Young, 2009) and 'learning friends' updates' (Hart et al, 2008) were key motivators. More traditional communication with others was also discovered to be an important reason for OSN participation by Young (2009) with 70% of respondents citing this reason. In addition to information sharing, only one study highlighted the capacity of information storage in OSNs as a motivation for participating (Lee et al 2008).

Clearly the distinctions between these motivational themes are not perfect. One might reasonably argue that 'keeping in touch with others', which was previously identified as a critical component to relationship maintenance, requires some level of information sharing. Thus, information seeking and sharing might rightly be additional components to relationship maintenance. Nonetheless, information sharing has been recognized as important to respondents from various geographical locations.

Social Discovery

Whether forming new relationships, otherwise known as social discovery, was a vital motivation for OSN participation was inconclusive. A 2009 public opinion poll from the United States revealed that approximately half of OSN users use these sites to make new friends (Lenhart, 2009), yet the literature reviewed did not demonstrate an equivalent level of support for this claim. Subrahmanyam et al (2008) reported only 29% of respondents used OSNs to find new friends and Young (2009) recorded only 13% of the same. However, making new friends was seen as an important reason for participating on Facebook when referring to the value others likely see in the site (Hoadley et al, 2010). Similarly, both studies by Acquisti and Gross (2006) and Hoadley et al (2010) revealed that finding dates were an important motivation for OSN use for others, but not for oneself. While these findings may signify a self-reporting bias as suggested by the authors, there is other evidence to suggest that Americans and individuals from other individualistic cultures do not use social networking sites for making new contacts, whereas individuals in collectivist cultures do.

In their international study of online social network users, Cardon et al (2009) discovered that survey participants from the United States, France, Israel and Sweden had the fewest online social ties that they had never met in person while participants from India, Turkey, Macao, China, and Thailand had significantly more. Similarly, in a study of Australian OSN users, it was revealed that only 2% of respondents cited the majority of their online friend networks were comprised of 'people I have never met', whereas 29% reported the majority of their online friends were people they spent time with offline and 23% reported the majority of their online friends were past colleagues or former school mates. Undergraduate students at an American university also indicated their primary use of Facebook was to connect with people they knew offline (mean=3.64 on a 5 point Likert scale) rather than to connect with new people (mean=1.97) (Ellison, Steinfield and Lampe, 2007).

The rise in popularity of Tagged, a social networking site that emphasizes social discovery, appears consistent with these observations. Tagged acquired hi5 in December 2011 bringing its registered membership to 330 million worldwide (Raice, 2011), however only about 30% of its user base is located in the individualist culture of the United States. Instead, Tagged remains popular in more collectivist nations including Southeast Asia, South America and a few European countries like Spain, Portugal and Romania (Raice 2011).

OSN Motivations Revealed through Uses and Gratifications Theory

Uses and gratifications (U&G) theory has been used to explain individuals' media consumption motives (Ruggerio, 2000) since at least the 1940s (Wimmer and Dominick, 1994). Essentially, this theory seeks to determine why audiences engage in certain types of media behaviour. Ruggerio (2000) presented an historical account of U&G theory within which he identified several criticisms including difficulties in generalising from results due to the emphasis on individuals, typologies of motives that were too compartmentalised, and the use of fuzzy concepts. As a result, the theory had fallen out of favour among some mass communications researchers, but Ruggerio (2000) argued that the advent of new computer-mediated communication technologies created an opportunity for increased application of U&G theory to establish benchmarks of motives for new media use.

Indeed, four of the twenty studies introduced in Table 2.4 utilized the U&G framework to determine user motives for OSN participation (Dholakia et al, 2004; Joinson, 2008; Cheung and Lee, 2009; Dunne et al, 2010). These studies represented a variety of perspectives drawn from samples of varying ages collected internationally, in the UK, Hong Kong, and Ireland, respectively. A summary of the varied findings with respect to motivations for OSN participation produced in this body of work is presented in Table 2.6.

As can be seen in Table 2.6, a variety of motives for OSN participation were concluded from research employing a U&G theoretical lens. Just as previous criticisms of U&G theory emphasised the compartmentalised typologies emerging from U&G based research, the results of these four studies demonstrated a similar issue. Although many of these motives may have identical or similar meanings, the inconsistency of language utilised in the research makes such a conclusion difficult. However, there did appear to be enough similarity in many of the specific motives identified that at least parallels could be drawn with the findings from exploratory approaches discussed in Section 2.3.2.1. Combined, these studies loosely revealed that relationship maintenance, self-presentation, entertainment, information, popularity and social discovery emerged as important motivations for OSN participation in various contexts.

Table 2.6 Motivations for OSN use within Uses and Gratifications Literature

Study	**Motivations for Using OSNs**	
Dholakia, Bagozzi and Pearo (2004)	1) entertainment value	
Joinson (2008)	1) social connection 2) shared identities 3) photographs 4) content 5) social investigation 6) social network surfing and 7) status updates	
Cheung and Lee (2009)	1) purposive value, 2) self-discovery, 3) entertainment value, 4) social enhancement, and 5) maintaining interpersonal connectivity	
Dunne, Lawlor and Rowley (2010)	*Gratifications sought* – 1) communication 2) friending 3) identity creation and management 4) entertainment 5) escapism and alleviation of boredom 6) information search 7) interacting with boys	*Gratifications Obtained* – 1) portraying one's ideal image 2) peer acceptance 3) relationship maintenance 4) safety from embarrassment and rejection 5) engaging in playground politics

From an exploratory factor analysis of 46 items, Joinson (2008) revealed seven distinct uses and gratifications of Facebook among a sample of young adults in the United Kingdom. Specifically, these included: i) social connection ii) shared identities iii) photographs iv) content v) social investigation vi) social network surfing and vii) status updates. Although empirically shown to be separate factors, these may be mapped loosely to correspond with the motivational themes identified through the exploratory research previously discussed such that photographs, content, and social investigation represent informational motivations, shared identities and status updates might be thought to pertain to self-presentation and social connection represents relationship maintenance.

Dholakia et al (2004) examined individuals' value perceptions of numerous virtual communities. While these authors were not specifically investigating online social networks, this study has been deemed important for inclusion because online social networks may have been included in the 'virtual communities' classification and also because this study served as foundational to subsequent studies of uses and gratifications in OSNs. Dholakia, et al (2004) hypothesized that individuals had five value perceptions that influenced participation in virtual communities. These value perceptions included i) purposive value - the value derived from accomplishing a pre-determined purpose; ii) self-discovery - the increased understanding of oneself gained through social interactions; iii) entertainment value; iv) social enhancement, or popularity; and v) maintaining interpersonal connectivity which is akin to 'relationship maintenance' conclusions from the exploratory studies previously mentioned. Of the five value perceptions examined, however, only entertainment value was found to be a significant predictor of virtual community participation.

In their 2009 investigation of user participation in a Hong Kong based OSN, Cheung and Lee were able to conclude that each of the five value perceptions initially hypothesized by Dholakia et al (2004) to influence virtual community participation did in fact influence participation in the OSN examined, but not directly. The relationships between purposive value and OSN participation and self-discovery and OSN participation were mediated by satisfaction; paths between social enhancement and OSN participation and maintaining interpersonal connectivity and

OSN participation were mediated by commitment; and all five value perception measures influenced group norms which in turn led to OSN participation.

Dunne et al (2010) furthered the research about uses and gratifications in OSN environments by distinguishing between the gratifications sought and the gratifications actually obtained from OSN use. In their investigation of Irish teen participation in the OSN Bebo, the authors concluded that their sample was generally seeking communication, friending, identity creation and management, entertainment, escapism and alleviation of boredom, information search, and interacting with boys. The gratifications obtained through Bebo usage included portrayal of one's ideal image, peer acceptance, safety from embarrassment and rejection, relationship maintenance, and engagement in playground politics.

OSN Motivations Revealed Through Social Capital Theoretical Approaches

This literature review revealed that five of twenty studies used social capital theory to frame their investigations (Lampe, Ellison and Steinfield, 2006; Ellison, Steinfield and Lampe, 2007; Steinfield, Ellison and Lampe, 2008; Pfeil, Arjan and Zaphiris, 2009; Valenzuela, Park and Kim, 2009), three of which were conducted by the same authors (Lampe, Ellison and Steinfield, 2006; Ellison, Steinfield and Lampe, 2007; Steinfield, Ellison and Lampe, 2008) and all but one of which was conducted in the United States (Pfeil, Arjan and Zaphiris, 2009). Each of the four studies using samples drawn from the US also relied entirely upon responses from university students and pertained exclusively to Facebook. As Facebook was the most popular OSN in the world at the time of writing, highly popular among university students and because it can be classified as a connection OSN that emphasized socializing (Beye et al 2010) its centrality in this research is fitting. However, the specificity of this research must be recognized and caution exercised in generalizing from it.

The investigation by Lampe et al (2006) suggested that social surveillance, the ability to “track the actions, beliefs and interests of the larger groups to which they [individuals] belong” (p. 167), is a critical function of Facebook that leads to the development of social capital. In this work, distinctions between two social surveillance behaviours were made based upon the kinds of social ties one maintained. Specifically, social searching - the investigation of people with whom one shares offline connections - was found to be a more important social surveillance activity than social browsing - the investigation of people and groups online with whom one would like to interact offline.

In assessing formation and maintenance of social capital of Facebook users, Ellison et al (2007) focused on three types of social capital including bridging social capital, bonding social capital, and maintained social capital. While bridging and bonding social capital were concepts well established within the social capital literature and introduced previously (Section 2.1.2), maintained social capital was a new type of social capital introduced by these authors. Maintained social capital refers to one’s ability to keep in touch with connections throughout life stages, particularly after physically disconnecting from a social network (Ellison, Steinfield and Lampe, 2007). It was concluded that strong associations between Facebook use and each type of social capital existed. Bridging social capital was found to be the most tightly linked with Facebook use, thereby supporting notions that information sharing and social surveillance are important reasons for participation in this OSN. Building on their earlier work, Steinfield, Ellison and Lampe (2008) subsequently revealed that Facebook facilitated social interaction and led to gains in one's bridging social capital.

Similarly, Valenzuela, Park and Kim (2009) showed that Facebook use was positively associated with three kinds of social capital as well. In this study, however, the authors examined three different domains of social capital and the relationship between intensity of Facebook use and social capital was investigated from a holistic perspective rather than that derived from OSN interactions. Using Scheufele and Shah's (2000) framework of social capital, Valenzuela et al (2009) revealed that intrapersonal social capital (life satisfaction), interpersonal social capital (trust among individuals), and behavioural social capital (active participation in civic and political activities) were positively associated with intensity of Facebook use, and though significant, the relationships were small. Further, as relationship causality was not investigated it was not established whether Facebook use intensity created social capital or whether those with more social capital more actively participated in Facebook.

As previously mentioned, most of the research on social capital in online social networks was directed at young people and utilized samples of undergraduate students in particular. One study that did investigate the social capital of older adults in OSNs was conducted by Pfeil, Arjan and Zaphris (2009). While specific measures of social capital were not collected, the authors' content analysis of MySpace profiles revealed differences in the types of social capital individuals might be able to access based upon the age of participant. This study concluded that a social capital divide existed among age segments with teenagers (aged 13-19 years) tending to have larger networks of similarly aged friends and older adults (60+ years) tending to have much smaller networks of diverse age ranges. Previous studies have shown bridging, bonding and maintained social capital were associated with OSN use (Ellison et al, 2007). But, bridging social capital exists among weak, diverse ties and bonding social capital exists among strong, close ties with individuals of shared backgrounds (Putnam, 2000). Implied in Pfeil, Arjan and Zaphris' (2009) results, then, was that younger OSN users might be better able to derive bonding social capital from their homophilus networks while older OSN users might be better able to derive bridging social capital due to the heterophilus connections.

Two other studies (Cheung and Lee, 2010; Cheung, Chiu and Lee, 2011) used social capital theory indirectly to conceptualize participation in online social networks. These studies specifically focused 'We-Intention' which has been explained as the ''commitment of an individual to engage in joint action and involves an implicit or explicit agreement between the participants to engage in that joint action" (Tuomela, 1995, p.9). Again, the use of differing terminology does not permit exact comparisons to be drawn with social capital theory, but clearly notions of social solidarity and cooperation are implicit in 'We-Intention'.

Cheung and Lee (2010) concluded that subjective norms predicted one's collective intention (We-Intention) to participate in OSNs. Thus, if one's acquaintances participate in OSNs and one identifies closely with that group of people, they would have a greater commitment to participate in those environments. In their subsequent study, Cheung, Chiu and Lee (2011) revealed that specific social factors influenced this collective, 'We' intention. Specifically, the authors investigated three types of social factors that might predict We-Intention – social presence, social influences (subjective norms, group norms and social identity) and five uses and gratifications of OSN participation (purposive value, self-discovery, entertainment value, social enhancement and maintaining interpersonal connectivity (Cheung and Lee, 2009). Social presence was found to be the strongest predictor of We-Intention. Among the social influences measured, only group norms was found to be a significant predictor of We-Intention. Among the five uses and gratifications, only three were found to be significant predictors of We-Intention among Facebook users: maintaining interpersonal connectivity, social enhancement and entertainment value.

Only one article within the literature review has gone unmentioned to this point. Palmer and Koenig-Lewis' (2009) research involved a completely different perspective from the other nineteen works identified in Table 2.4, yet also asserted the connection between social capital and OSN participation. Whereas all the other studies involved primary data collection and discussed OSN participation and motivations from a general perspective, Palmer and Koenig-Lewis presented a conceptual model for *consumers'* OSN participation. Essentially, these authors suggested that consumers use OSNs to facilitate purchase decision making, for reputational and social identity reciprocity achieved through active participation, and 'flow' (a experiential state so desirable that one wishes to replicate it as often as possible) achieved through continued use of an OSN to progressively find new information or challenge established ideas.

Connections to Social Capital from all Research Approaches Combined

While some researchers have explicitly grounded investigations of OSN participation motives directly within social capital theory, there were apparent connections between individuals' motivations for OSN participation and concepts commonly associated with social capital revealed through research approaches guided by alternative theoretical orientations.

Social capital has been conceived as both a cause and an effect of social interaction (Resnick, 2002; Williams, 2006; Ellison, Steinfield and Lampe, 2007). Thus, social capital may result from OSN participation but the potential for social capital may also serve as the ultimate motivation to participate. Many of the individual motivational themes revealed through exploratory research approaches discussed in this section (Section 2.3.1) might rightly reflect social capital desires. For instance, we might join OSNs to 'keep in touch' or to 'socialize' or for 'intimacy' but do we not do these things to ultimately acquire some caché among those connections? Likewise, social capital may be an outcome of information sharing and seeking, for if we provide information and acquire information about others, does that not increase our bonds (and thus social capital) with those connections? Even still, social capital can be thought of as an outcome of our popularity, the friends we make (social discovery) and the self-presentations and the identities we construct in OSNs.

Other than the entertainment motive identified, all motives for OSN participation revealed through exploratory research approaches have clear links to social capital theory. Social relations have been established to be a fundamental component of social capital (Coleman, 1988; Newton, 1997; Nahapiet and Ghoshal, 1998; Woolcock, 1998; Paldam, 2000; Putnam, 2000), thus relationship maintenance motives and the other motives pertaining to strengthening and developing social relations likewise suggest social capital.

Relationship maintenance was consistently identified as a motivation for OSN participation, but there were distinctions in the types of relationships sought in these online communities. It appeared from this group of studies that social discovery, or bridging social capital, was not the most important type of connection sought within OSNs (Subrahmanyam et al, 2008; Young, 2009). Instead, OSN users sought relationships with those they already maintained an offline connection, thus bonding social capital or maintained social capital may be implied.

Within the social capital literature, information access has been identified as a crucial benefit (Coleman, 1988; Burt, 1992). Specifically, Nahapiet and Ghoshal (1998) espoused the idea that the strong, symmetrical ties associated with affective relationships influenced individuals' motivation to engage in social interaction and knowledge exchange. Therefore, the studies herein that specified information as an important motive for OSN participation can be argued to be social capital motives.

Though varied typologies of uses and gratifications of OSN use were provided in the reviewed studies, there were similarities with results from exploratory approaches (Joinson, 2008; Dunne et al, 2010). Combined, these studies revealed that relationship maintenance, self-presentation, entertainment, information, popularity and social discovery emerged again as important motivations for OSN participation in various contexts. Thus, these concepts may be similarly connected to social capital.

The literature using U&G theory also revealed other interesting connections to social capital. Specifically, Cheung and Lee (2009) identified that each of the uses and gratifications of OSN participation were not direct influences on participation. Instead, each was mediated by another variable that demonstrated clear connections with social capital theory.

First, obligations were recognised as critical to social capital by Coleman (1988) and commitment was expressed as a dimension of social capital Putnam (1995a; 2000). Commitment is reflective of social relations in that it provides an indication of the strength of ties among group members. According to Cheung and Lee (2009), commitment was found to be necessary to mediate relationship maintenance and social enhancement uses and gratifications. Thus, one component of social capital was shown to be directly related to OSN participation.

Second, group norms had been identified as an important relational component of social capital (Nahapiet and Ghoshal, 1998; Newton, 1998). From Cheung and Lee (2009) we learned that all five uses and gratifications - purposive value, self-discovery, entertainment value, social enhancement and relationship maintenance – influenced group norms which in turn influenced OSN participation. Thus, Cheung and Lee (2009) established that among their sample, another component of social capital was directly derived from OSN motivations.

2.4 Concluding Remarks

Individuals clearly engage in OSNs for social capital. Research has identified that three kinds of social capital - bringing, bonding and maintained - were all motives for OSN participation. Other research, guided by different theoretical orientations, has highlighted a variety of specific reasons for OSN participation including relationship maintenance, social surveillance, social discovery, social capital, and social presence. The review of studies employing both a uses and gratifications theoretical framework and those adopting ungrounded exploratory approaches has clearly illustrated that many of the OSN motivations identified in the literature were social in nature. While not identified specifically as social capital motivations, one might realistically infer that they could be considered as such because numerous motivations identified serve to reinforce social relations -an essential dimension of social capital (Coleman, 1988; Newton, 1997; Nahapiet and Ghoshal, 1998; Woolcock, 1998; Paldam, 2000; Putnam, 2000). Also, as Nahapiet and Ghoshal (1998) point out, "social relations, often established for other purposes, constitute information channels that reduce the amount of time and investment required to gather information" (p. 252) and thus the social capital inherent in the social relations is appropriable (Coleman, 1988). Further supporting claims that the specific motivations identified through various theoretical lenses were appropriately connected with social capital, Cheung and Lee (2009) were able to provide empirical evidence linking various uses and gratifications of OSN participation with constructs commonly used in social capital research – group norms and commitment. Thus, we are able to conclude from this literature review that OSN participation is motivated by social capital in some way.

Each of the motivations discussed herein relates to positive benefits of OSN participation. However, despite there being numerous social benefits influencing individuals' decisions to participate in OSNs, one's participation does not occur in the absence of risk. OSN participants are particularly vulnerable to privacy violations in OSNs because of the nature of the environment and the desire to achieve social capital is dependent upon sharing personal information.

First, the overview of OSNs presented in Sections 2.2.1 and 2.2.2 of this document emphasised that one feature of OSN participation is the requisite sharing of personal information. The construction of a public or semi-public profile, articulation of a list of friends, and the supply of various pieces of personal information allows one to achieve an assortment of social goals. There is typically no financial cost to join most of the world's top OSNs. Instead, the only thing one must be willing to provide, or the price of membership, is essentially one's personal information. While the user maintains some discretion about the type of information shared and, depending on the OSN, may retain varying degrees of control over which members of the network can access their information, some information disclosure is necessary to first participate.

Second, integral to social capital is information flow (i.e. Coleman, 1988; Nahapiet and Ghoshal, 1998) and many studies reviewed herein also identified the importance of information as a motivation to OSN participation. It is conceivable, then, that individuals might expect greater social benefits such as relationship maintenance, popularity and/or social capital to accrue as the amount of personal information one shares increases. But, Sandefur and Laumann (1998) cautioned that the information benefit associated with social capital carries with it a liability of privacy. For, sharing too much highly personal, sensitive and potentially stigmatizing information can reduce social benefits (Nosko, Wood and Molema 2010). Ellison, Steinfield and Lampe, (2007) similarly cautioned that information exchanges in OSNs leave users open to privacy abuses. And, in our OSN dominated world, Andrew Keen lamented, “privacy...is being dumped into the dustbin of history” (Keen, 2012).

Thus, privacy must be a critical consideration with respect to social capital in OSNs. Accordingly, the topic of privacy in OSNs will be addressed in Chapter 3.

3 Privacy

3.1 Privacy

The concept of privacy has been argued to be an important concern within OSNs (Ellison, Steinfield and Lampe, 2007) and a noted liability of information benefits of social capital (Sandefur and Laumann, 1998). But what does 'privacy' really mean? The concept of privacy may have enjoyed a long history of academic attention but there is not one simple answer to that question. Section 3.1 of this Project will present a discussion of what privacy entails by first considering the value of privacy as discussed in the literature (Section 3.1.1), present the various definitions suggested for the construct (Section 3.1.2) and then discuss the contextual nature of privacy (Section 3.1.3) with particular emphasis on consumer online information privacy.

3.1.1 The Value of Privacy

"Privacy is like freedom: we do not recognize its importance until it is taken away."

(David Flaherty *in* Cavoukian and Hamilton, 2002)

The notion that privacy is valuable has been well supported in the literature (Moore, 2003). Alan Westin's *Privacy and Freedom* (1967) has been the most frequently cited work on the issue of an individual's information privacy and has been considered a seminal work. In his comprehensive evaluation of the conflict between privacy and surveillance, Westin contended that there is indeed a social value to privacy and subsequently provided a detailed description of four functions that privacy performs. According to Westin, privacy’s value lies in its ability to afford one i) personal autonomy over whether and when to make personal information public, ii) emotional release or freedom from public role playing, iii) time for self-evaluation and iv) the freedom for limited and protected communication. These benefits represent a psychological perspective of the value of privacy similarly asserted by Margulis (2003). For his part, Margulis (2003) argued that the value privacy provided was in the positive psychological development, individuality and autonomy of the individual.

However, Margulis (2003) was also careful to discern his contention that while the benefits of privacy might belong to an individual, privacy is a social phenomenon in that it is both social psychological and social-political. Schwartz (1968) also provided a noteworthy account of the value of privacy in social psychology. Specifically, Schwartz believed that privacy was a universal phenomenon carried throughout human evolution and was valuable because it: i) was group-preserving, ii) maintained status divisions, iii) allowed for deviation, and iv) sustained social establishments.

Other arguments in support of the value of privacy tend to link privacy with intimacy and social relationships. In particular, Fried (1970), Gerstein (1978), Schoeman (1984) and Inness (1992) have argued that privacy is necessary to form intimate relationships. Fried (1970) contended that privacy has intrinsic value because friendship, love and trust were impossible to achieve without it and, therefore, privacy is fundamental for intimacy. Gerstein (1975) argued that privacy is valuable in that it permits intimacy in communication and interpersonal relationships thereby allowing individuals the freedom to truly experience their lives with spontaneity and without shame. Schoeman (1984) extended the argument of privacy's value beyond intimacy by asserting that the benefits associated with the condition of privacy include not only intimacy in social relationships but also permit one's personal development. In her discussion of privacy from the perspective of invasions on that condition, Inness (1992) argued that privacy affords one the ability to protect both intimate information and activities so that one's loving and caring needs may be fulfilled. And, while Rachels (1975) similarly argued that privacy was necessary for social relationships, he also maintained that those relationships need not only be of an intimate nature. Whereas most of the authors cited in this section have defended views of privacy referring to control over information, Rachels' contention was that privacy also included control over *access* of any kind to oneself.

Privacy was also argued to hold value in relationships not only for the positive benefits of friendship, love and trust but for its necessary role in protecting the power balance of relationships. As Parent (1983) wrote, "if others manage to obtain sensitive personal knowledge about us they will by that very fact acquire power over us" (p. 276). And, privacy does not only serve to protect a power balance within social relationships, it may also protect from abuses of power from organisations including governments and business (Schneier, 2011). In our 'surveillance society' (Lyon, 1994) where precise details of our personal and consumer lives are held within massive databases controlled by governments and big corporations, "Privacy protects us from abuses by those in power, even if we're doing nothing wrong at the time of surveillance" (Schneier, 2011: http://www.wired.com/politics/security/commentary/securitymatters/2006/05/70886)

Despite these value arguments, there are others who argue privacy may not have value because it is not a distinct concept. Both Schoeman (1984) and The Stanford Encyclopedia of Philosophy (2012) distinguished different schools of thought about privacy. According to the Stanford Encyclopedia of Philosophy, 'coherentists', like those previously mentioned, have argued that there is something distinct, coherent and valuable about privacy interests. Conversely, 'reductionists' including Judith Jarvis Thomson (1975) and Richard Posner (1981) were more sceptical of privacy and have argued the opposite about the distinctiveness of the construct. Reductionists contend that any discussion of what some refer to as 'privacy' can be reduced to more basic claims such as those against personal property or inducement of emotional distress (Thomson, 1975) and that privacy tends to be protected in economically inefficient ways (Posner, 1981). Reductionists' criticisms of privacy are not that personal information or activities should not be protected so much as that they can be protected more efficiently or more appropriately when classified according to their more basic claims.

Unlike reductionists, there are true privacy sceptics who argue that privacy simply has no value in a digital age where personal information is readily available, accessible and can be compiled from a variety of sources. Most widely acknowledged comments to this effect have been attributed to those heading large technologically driven companies or social media analysts. In other words, those with much to gain from the masses believing that privacy has no value and is not worth protecting tend to be vocal opponents. Sun MicroSystems CEO Scott McNealy is widely credited with this brazen assertion, "Privacy is dead, deal with it." (Meeks, 2000). Marc A. Smith, from the Social Media Research Foundation, claimed that “Nothing is private” (Lipschultz, 2012). And, perhaps most telling were Facebook CEO Mark Zuckerberg’s comments made in 2010, “People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time." (*in* Johnson, 2010).

However, given the same circumstances - that in the digital age personal information is readily available, accessible, replicable and can be compiled from a variety of sources – privacy may be even more valuable than ever. Clearly, there are sufficient arguments defending the value of privacy in social relationships. And, as has been extensively developed in Chapter 2, social benefits were clearly established as the primary reasons for which individuals participate in OSNs. Therefore, if privacy is necessary to achieve social benefit and the personal information that is so readily available and accessible on OSNs exists because of users’ desires for social benefit, that same availability and accessibility of personal information on OSNs creates a vulnerability to privacy, thereby making privacy in OSNs paramount for users.

3.1.2 Privacy Defined

Isolating a commonly accepted definition of privacy has eluded scholars since the first published definition of the concept appeared in 1890 (Warren and Brandeis). Philosophical debate about the construct surged in the 1960s (Schoeman, 1984; DeCew, 1997) but failed to result in a codified presentation of the construct. Academic study of the concept has appeared in a variety of disciplines including philosophy (Schoeman, 1984; DeCew, 1997), psychology (Stone et al., 1983); sociology (Westin, 2003), law (Solove, 2006) and business. Investigations of privacy in a number of specific business contexts including direct marketing (Goodwin, 1991; Nowak and Phelps, 1992; Culnan, 1993; Culnan and Armstrong, 1999), information systems (Smith, Milberg and Burke, 1996; Stewart and Segars, 2002), e-commerce (Malhotra, Kim and Agarwal,, 2004; Liu et al, 2005; Eastlick, Lotz and Warrington, 2006; Xu et al, 2008) and online social networks (Aquisti and Gross, 2006; Krasnova & Veltri, 2010; Krasnova et al, 2010) have also been conducted. Despite its long history of study, recent scholars admit to being unable to agree upon a commonly accepted definition of privacy (Introna and Pouloudi, 1999; Margulis, 2003; Casteñeda, Montoso and Luque, 2007) or whether, as discussed in the previous section, the concept of privacy as a distinct construct even exists (Jarvis Thomson, 1975). However, as there have been more philosophical arguments representing privacy as a distinct construct than not, arguments for a reductionist view of the construct have been highly criticized (Inness 1992), and there remains common acceptance of a notion of 'privacy', the remainder of this discussion will primarily focus on coherentist thought wherein privacy is believed to be distinct and valuable.

Though Warren and Brandeis (1890) have often been credited with laying the foundation of the concept of privacy, other writers, including English philosopher James Fitzjames Stephen, questioned the meaning of the concept even earlier. In his, *Liberty, Equality and Fraternity* (1873), Stephen wrote, "To define the province of privacy distinctly is impossible, but it can be described in general terms". Well over a century later, similar assertions have been made, including:

- “Privacy is an elastic concept.” (Allen, 1988)
- “The concept of privacy is a widely accepted legal and moral notion but has uncertain legal and philosophical foundations.” (Moor, 1990, p. 69)
- “Many commentators have sought to bring greater specificity to the concept of privacy, yet it seems that each privacy commentator forwards a different definition of privacy and at least five reasons why every other definition is inadequate.” (Craig, 1997)
- “Despite the fairly intense debate since the late 1960s there is still no universally accepted definition of privacy.” (Introna and Pouloudi, 1999).
- “Adequately defining privacy raises problems” (Margulis, 2003).
- “It is apparent that the word ‘privacy’ has proven to be a powerful rhetorical battle cry in a plethora of unrelated contexts … Like the emotive word ‘freedom’, ‘privacy’ means so many different things to so many different people that it has lost any precise legal connotation that it might once have had.” (McCarthy, 2005)
- “Privacy is a concept in disarray. Nobody can articulate what it means.” (Solove, 2006, p. 477)

According to Schoeman (1984), three themes have typically been represented in philosophically rooted privacy literature - privacy definition, privacy’s centrality to morality, and moral scepticism over its value. Concentrating on the literature dedicated to privacy definition, the task of clarifying the meaning of the construct does not become much easier, however, as numerous nuanced definitions have been presented. Perhaps most clearly revealing the excessive variation in privacy definitions was Katherine J. Day's (1985) doctoral dissertation from the University of Edinburgh, "Perspectives on Privacy: A Sociological Analysis" in which more than one hundred privacy definitions were provided (Science Encyclopedia, n.d.). And, as illustrated previously, debate over privacy definitions has continued. Therefore, in order to first make sense of privacy from a conceptual perspective, some commonly cited definitions are reviewed (Table 3.1).

Table 3.1 Examples of Privacy Definitions

Author	**Definition**
Warren and Brandeis (1890)	"The right to be let alone"
Prosser (1960)	Privacy is composed of four separate torts. "Without any attempt to exact definition, these four torts may be described as follows: 1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs. 2. Public disclosure of embarrassing private facts about the plaintiff. 3. Publicity which places the plaintiff in a false light in the public eye. 4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness" (p.389)
Westin (1967)	"Privacy is the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about themselves is to be communicated to others."
Fried (1970)	"Privacy is not simply an absence of information about us in the minds of others, rather it is the *control* we have over information about ourselves". (p.209)
Parker (1974)	Privacy is control over when and by whom the various parts of us can be sensed by others.
Altman (1975)	Privacy is the selective control of access to the self
Gavison (1980)	Privacy is a complex of three independent and irreducible elements: secrecy (the extent to which an individual is known), anonymity (the extent to which an individual is the subject of attention), and solitude (the extent to which others have physical access to an individual).
Stone et al (1983)	"the ability (i.e., capacity) of the individual to control personally (vis-à-vis other individuals, groups, organizations, etc)

	information about oneself."
Parent (1983)	“[Plrivacy is the condition of a person’s not having undocumented personal information about himself known by others”. (p.346)
Solove (2006)	“The term “privacy” is an umbrella term, referring to a wide and disparate group of related things.” (p. 485) “In the taxonomy that follows, there are four basic groups of harmful activities: (1) information collection, (2) information processing, (3) information dissemination, and (4) invasion. Each of these groups consists of different related subgroups of harmful activities.” (p. 488)

Although differences were evident among these definitions, it was also clear that they tended to either describe privacy as a distinct right (Warren and Brandeis 1890), as control over personal information (Westin 1967; Fried 1970; Parker 1974; Parent 1983; Stone et al 1983), or as restricted access (Parker 1974; Altman 1975; Gavison 1980). And, while both Solove (2006) and Prosser (1960) argued that there were distinct types of harmful activities that fall under the umbrella of privacy and ultimately require legal protection, close inspection of those harms revealed that each of Prosser’s four torts and Solove’s four basic groups of harmful activities might be argued as capable of protection via control over personal information by coherentists.

Similarly, Schoeman (1984) summarised privacy definitions as either i) a right to determine what information about oneself to reveal, ii) a measure of the control one has over personal information and sensory access to oneself, or iii) a state of limited access to a person. Consistent with these assessments was Moor’s (1990) argument that three classes of definition exist – those that explain privacy as i) control over personal information, ii) undocumented personal knowledge, or iii) restricted access. While Moor’s classification of privacy definitions separated Parent’s (1983) definition into a class to itself wherein undocumented personal information is protected, the classifications of each of these authors clearly signified that there was support for a view of privacy as control over personal information (documented and or undocumented) and restricted access.

Whether privacy constitutes a ‘right’ depends much upon the context of the discussion and was beyond the scope of this analysis. As the purpose of this investigation is to examine privacy from a consumer context, the emphasis focussed on ‘privacy’ as a consumer attitude and, as a result, privacy as either restricted access or control over personal information emerged as important considerations. Thus, each of these views of privacy will be discussed next.

Restricted Access

Privacy defined as restrictive access (Parker, 1974; Altman, 1975; Gavison, 1980) takes a broad view of the concept where access refers to access to the entire self. Such a view tends to look at privacy as inclusive of personal property, one’s physical body and also personal information. Utilizing this rationale, Gavison (1980) argued that privacy was comprised of three independent and irreducible elements: secrecy (the extent to which an individual is known), anonymity (the extent to which an individual is the subject of attention), and solitude (the extent to which others have physical access to an individual). Allen (1988), too, discussed privacy from the perspective of restricted access to the person. Similarly, Julie Inness (1992) crafted a comprehensive definition of privacy from analysis of US legal torts which resulted in three types of privacy – access to intimate aspects of the agent’s person (‘restricted access’), access to intimate information about the agent (‘information privacy’), and autonomy in the agent’s decisions about intimate matters (‘decisional privacy’). Though inclusive, the breadth of coverage in these kinds of definitions tended to become problematic when discussing exactly what was meant by a term as comprehensive as ‘privacy’. Thus, others have constrained definitions further to concentrate upon personal information and one’s control of it.

Control over Information

Building upon the legal discussion of privacy by Warren and Brandeis, Prosser’s (1960) view of privacy was based upon seventy years of U.S. tort review. Though not claiming to be an exact definition of privacy, four definite invasions of privacy did emerge from his analysis, namely:

1. Intrusion upon a person's seclusion or solitude, or into his private affairs.
2. Public disclosure of embarrassing private facts about an individual.
3. Publicity placing one in a false light in the public eye.
4. Appropriation of one's likeness for the advantage of another (Prosser 1960, p.389).

And, as each of these invasions envisioned by Prosser pertained to personal information about the individual, one might be argued to have established privacy when they are able to maintain control of their information to prevent such invasion.

Similarly, Westin (1967) described privacy as the ability to determine for oneself when, how and to what extent information about one is shared with others. Whereas legal scholars such as Prosser tended to focus their discussions of privacy from protectionist perspectives via judgements about privacy violations deemed to have occurred in American law, others including Westin (1967) assumed a different perspective approaching discussions from the beneficial functions privacy performs. Westin’s view was consistent with the aforementioned contention that privacy pertains to ‘control over information about oneself’ and clearly defined the value of privacy by way of four separate benefits previously mentioned - personal autonomy, emotional release, self-evaluation and limited and protected communication.

Though Parent’s (1983) definition of privacy related to information privacy as well, he focused on the source of the information in his definition, “privacy is the condition of a person’s not having undocumented personal information about himself known by others” (p. 346). Unlike others’ emphasis on legal rights to privacy, Parent concentrated his argument on the moral value of privacy when he argued that factual personal information as a matter of public record could be acquired and shared without being considered a violation of privacy.

More recently, Solove (2006) presented a new taxonomy of privacy from a legal perspective. Like Prosser (1960), Solove argued that privacy was multidimensional and rather than pursue a top-down approach to defining the construct, privacy should be conceptualised via anticipation of “the specific types of disruption and the specific practices disrupted rather than looking for the common denominator that links all of them” (Solove, 2002, p. 1130). Whereas many of Solove’s predecessors in legal privacy writing constrained their thinking to an individual’s dignitary harms that could result from privacy violations, Solove extended the list of disruptions to a more modern context that incorporated ‘architectural’ harms. As a result of the proliferation of electronic information and increasing digitization of the consumer, Solove argued that dignitary harms are not the only violations of privacy that may occur against a person. His taxonomy (2006) specified four basic groups under which harmful activities to an individual might result by way of invasions of privacy. These included: i) information collection ii) information processing iii) information dissemination and iv) invasion.

Burgoon et al (1989) and DeCew (1997) discussed multidimensional definitions of privacy as well. Burgoon et al (1989) identified that privacy was “the ability to control and limit access to the self or one’s group” (p. 132) on four dimensions, namely: i) physical dimension, ii) interactional dimension, iii) psychological dimension and iv) informational dimension. DeCew (1997), on the other hand, while also presenting a multidimensional view of the construct, specified different dimensions within the domain of privacy. Namely, DeCew (1997) identified an informational dimension, an accessibility dimension and an expressive dimension. These definitions incorporated both the control and access considerations of definitions previously presented and also illustrated the importance of recognising the informational dimension as a distinct consideration of privacy and a basis upon which investigations may be constrained.

What can be gleaned from the discussion of privacy definitions thus far is that, among those accepting privacy as a value, the privacy construct is complex and is likely best represented multidimensionally. The arguments presented also illustrated that the privacy construct becomes more easily understood when constraints are placed upon the definition consistent with one of its dimensions. Privacy has been defined inclusively as restricted access or more narrowly as control over personal information, but privacy of information was a distinction that consistently emerged in most discussion of the construct. Although there was some suggestion that defining ‘personal information’ might also introduce complexity

(Parent 1983), information privacy was clearly a narrow, manageable, well accepted view of the construct.

However, a definition of privacy narrowed to the 'information' parameter may not be sufficiently constrained, as Wasserstrom (1978) argued, "information about oneself is not all of the same type. As a result, control over some kinds may be much more important than control over others" (p.317 *in* Schoeman (ed.), 1984). Furthermore, it was also observed in the course of this literature review that technological developments have encouraged more evolved definitions of the privacy construct (Solove, 2006). As such, the next section of this literature review will discuss the contextual nature of privacy to arrive at an appropriate level of constraint for investigation of privacy in online social networks.

However, before proceeding, a distinction between information privacy and other closely related constructs was also necessary. In their comprehensive review of information privacy literature, Smith, Dinev and Xu (2011) clearly articulated that information privacy is ***not*** anonymity, secrecy, confidentiality, security nor ethics despite Gavison's (1980) claims to the contrary.

Anonymity limits identifying information from being linked back to an individual either completely in anonymous situations or partly in pseudonymous situations. Though anonymity can be clearly interrelated with privacy, it was argued to be distinct (Camp, 1999; Smith, Dinev and Xu, 2011). Secrecy refers to the intentional concealment of information. Secrecy was considered different from privacy as it entails hiding more information than what is necessarily private (Bok, 1989; Smith, Dinev and Xu, 2011). Further, Smith, Dinev and Xu (2011) argued that confidentiality is also distinct from privacy because whereas "[p]rivacy corresponds to the desire of a person to control the disclosure of personal information; confidentiality corresponds to the controlled release of personal information to an information custodian under an agreement that limits the extent and conditions under which that information may be used or released further." (p. 996). Drawing on arguments from Culnan and Williams (2009) and Ackerman (2004), Smith, Dinev and Xu (2011) subsequently contended that privacy is not security. Particularly, it was argued that while security is a necessary condition for privacy to exist, it is insufficient to describe privacy. For instance, an organization may keep a customer's information secure, but make poor decisions with the use of the information thereby violating that customer's information privacy. Finally, while Smith, Dinev and Xu (2011) acknowledged that there are clearly ethical dimensions of privacy notably presented in a number of works including Ashworth and Free (2006), Caudill and Murphy (2000), Culnan and Williams (2009), and Foxman and Kilcoyne (1993), they contended that equating privacy with ethics was inappropriate and that empirical research into the construct may reasonably be undertaken in the absence of ethical considerations of the construct.

3.1.3 Contextual Nature of Privacy

While privacy has been shown to be supported as something of value in the previous sections of this review and several common notions associated with the construct were evidenced, there remain unresolved questions about the universality of the construct. We have seen that narrow definitions of the construct were considered more manageable and ‘information privacy’ appeared to be a nicely defined parameter of discussion. However, we have also questioned whether that definition could be narrowed further especially given that personal information is not all of the same kind and technological developments such as OSNs are changing the ways that personal information is communicated. Indeed, Vasalou et al (2011) declared, “Despite theorists’ argreement over several shared features, *context* determines much of the way that privacy has been defined” (p.7). Accordingly, this section will therefore address the arguments for a contextual nature of privacy and conclude with the argument that discussing privacy in terms of ‘online consumer information privacy’ was an appropriately narrowed concept for this investigation.

Westin’s (1967) definition of privacy as control over personal information has been commonly acknowledged in business literature, and while he argued for such a narrowed definition of the construct, he did not argue that privacy was an absolute condition. Essentially, Westin suggested that there were four states of privacy – solitude, intimacy, anonymity and reserve[7] – and one person may experience different states given the context of a situation. Suggesting that one may have different privacy requirements about their personal information in various situations, an individual might experience one state in a given circumstance but that same individual might experience a different state in a differing circumstance.

[7] Solitude refers to an individual being separated from the group and freed from the observation of other persons; Intimacy refers to the individual is part of a small unit; Anonymity refers to freedom from identification and surveillance though the individual is in public; Reserve refers to withheld communication as a psychological barrier against intrusion.

Privacy has also been argued to be culturally relative (Westin, 1967; Moore, 2003). Westin (1967) argued that privacy does not exist in the same forms across cultures but is dependent on rules and social norms within cultures. Similarly, Moore (2003) argued that privacy is culturally relative concept and dependent upon economic, political and technological variables.

From a consumer perspective, Goodwin (1991) similarly offered an oft-cited conceptualisation of privacy that further supports the notion that privacy is indeed contextual. In her description of the construct, she theorized four privacy states based upon the degree of control one has over both disclosure of their information and the physical presence of others in a market transaction. According to her 2x2 matrix taxonomy of privacy states, one has 'no control' if they have low control over information disclosure and low control over the presence of others in the market transaction, conversely, one has 'total control' under opposite conditions. One is considered to have 'environmental control' if they maintain high control over the physical presence of others in the transaction but low control over information disclosure. Finally, one has 'disclosure control' when a situation of high control over information disclosure and low control over presence of others in the transaction occurs.

In Goodwin's (1991) work, the contextual nature of the privacy construct was clearly recognized, but the specific contextual conditions described may have changed since the time of development. If we accept that privacy is contextual, as argued thus far, and if we accept that privacy is dependent upon the environment in which a transaction occurs as argued by Goodwin, transactions that occur online must be treated as a distinct context because Goodwin's conceptualisation was presented prior to common adoption of the Internet and only went so far as to account for the 'physical presence' of others in the transaction. Furthermore, consistent with arguments that digital information communication technologies (ICTs) such as OSNs can alter both the nature of informational privacy and our understanding of it (Floridi, 2005) and that new architectural privacy harms are present in electronic information environments (Solove, 2006), privacy in OSNs should be treated as a distinct context as well.

Finally, as marketing research maintains an emphasis on the consumer and most business research on privacy tends to emphasise individuals' privacy attitudes or *concerns,* rather than the broader idea of privacy (Stone et al, 1983; Nowak and Phelps, 1992, 1995; Smith, Milberg and Burke, 1996; Culnan and Armstrong, 1999; Phelps, Nowak and Ferrell, 2000; Phelps D'Souza and Nowak, 2001; Stewart and Segars, 2002; Rose, 2005), this investigation will retain that definitional constraint.

Despite the lack of agreement on exactly what constitutes privacy, it has been shown that there are strong arguments in support of contextual definitions of privacy. To alleviate some of the philosophical complexity previously illustrated, researchers have tended to adopt increasingly narrow, discipline-specific definitions of the privacy construct by specifying situational and contextual constraints such as 'online', 'consumer' and 'information' to describe different types of privacy being investigated. As such, the remainder of this work will discuss privacy in the context of consumer concerns about their information privacy in online environments. The next section, then, will take the reader through an overview of consumer online information privacy concern from the perspective of academic research and public opinion research.

Consumer Online Information Privacy Concern

To understand consumer online information privacy, academic literature meeting the following selection criteria were reviewed: 1) a consumer perspective was captured; 2) an online focus in its measurement of privacy concern was specified; 3) a quantitative research approach was employed; 4) primary data was collected; 5) theory guided research was undertaken and 6) factor analysis of consumer online information privacy concern was included or consumer privacy concern was placed within an empirically tested nomological network. Given these boundaries, 16 empirical studies of consumer information privacy in online environments published between 1999 and 2010 were isolated (Table 3.2).

Table 3.2 Empirically Supported Factor Structure of Consumer Online Privacy Concern

Study	**Privacy Concern Conceptual Source**	**Privacy Concern Construct**	**Factor Specification**
Sheehan and Hoy (1999)	Nowak and Phelps (1992)	Total Concern	n/a
Sheehan and Hoy (2000)	Nowak and Phelps (1992)	Total Concern	1.Control over collection and use of information (6 items)
			2.Short term transactional relationship (5 items)
			3.Established long term relationship (3 items)
Bellman et al (2004)	Smith, Milberg and Burke (1996)	CFIP	1.Collection (4 items)
			2. Unauthorized secondary use (4 items)

			3. Improper Access (3 items)
			4. Errors (4 items)
Dinev and Hart (2004)	Smith, Milberg and Burke (1996); Culnan and Armstrong (1999); author created	Privacy Concern	1. Privacy concern for information finding (PCIF) (9 items)
			2. Privacy concern for information abuse (PCIA) (4 items)
Malhotra, Kim and Agarwal (2004)	Smith, Milberg and Burke (1996); author created	Internet User Information Privacy Concern (IUIPC)	1. Awareness of privacy practices (3 items)
			2. Collection (4 items)
			3. Control (3 items)
Dinev and Hart (2006a) (2006b)	Dinev and Hart (2004)	PCIA	PCIA (4 items)
Eastlick, Lotz and Warrington (2006)	Milne and Boza (1998); author created	Privacy Concern	Privacy Concern (4 items)
Van Slyke et al (2006)	Smith, Milberg and Burke (1996)	CFIP	1. Collection (4 items)
			2. Unauthorized secondary use (4 items)
			3. Improper Access (3 items)
			4. Errors (4 items)
Buchanan et al (2007)	Extensive combination of 45 items; Malhotra, Kim and Agarwal (2004)	General Internet Privacy Concern	General Internet privacy concern (16 items)
Casteñeda, Montoso and Luque (2007)	Culnan (1993)	General Online Privacy Concern	1.Concern for control over collection of personal information (4 items)
			2. Concern for control over use of personal information (4 items)
		Merchant Specific Online Privacy Concern	1. Concern for control over collection of personal information (2 items)
			2. Concern for control over use of personal information (2 items)
Moscardelli and Divine (2007)	Nowak and Phelps (2000); Sheehan and Hoy (1999)	Privacy Concern	Privacy Concern (14 items)
Lian and Lin (2008)	Smith, Milberg and Burke (1996)	CFIP	1. Collection (4 items)
			2. Unnamed (10 items)
Xu et al (2008)	Smith, Milberg and Burke (1996)	Privacy Concern	Privacy Concern (5 items)
Krasnova and Veltri (2010)	Dinev and Hart (2006)	Privacy Concern	Privacy Concern (4 items)
Li, Sarahathy and Xu (2010)	Smith, Milberg and Burke (1996); Malhotra, Kim and Agarwal (2004)	Global Information Privacy Concern	Privacy Concern (3 items)

Examination of these studies revealed some noteworthy findings relevant for discussion herein. (A detailed review is found in Morrison, 2011.) First, although the reviewed studies commonly drew upon consumer information privacy concern constructs established in research conducted offline, there was considerable diversity in the source conceptualisations utilised. Second, despite the selected literature meeting the rigid selection criteria stated above, the identified studies failed to produce a singularly accepted conceptualization of the construct of interest. While this was most likely a result of the diversity of source conceptualisations, this conclusion highlights the difficulty of comparing research about consumer online information privacy concerns. For, in order to advance scientific inquiry of complex constructs such as consumer privacy concern and its relationships with consumer behaviour, ‘it is essential that the scientific community use similar operative definitions and measurement instruments for the variables analysed’ (Casteñeda, Montoso and Luque, 2007, p.421; Day and Montgomery, 1999) because ‘pursuing empirical work before adequately defining concepts is like putting the cart before the horse’ (McKnight and Chervany, 2002, p.36). Therefore, understanding the various privacy concern conceptualizations that have been utilized in the rapidly evolving online environment where technology developments consistently outpace conceptual understanding was a necessary step on the path of rigorous scientific research of online consumer information privacy concern.

Conceptualisations of Consumer Online Information Privacy Concern

While no one conceptualisation has been consistently employed, review of these sixteen studies does suggest a widespread acceptance of Smith, Milberg and Burke’s (1996) rigorously developed Concern for Information Privacy (CFIP) construct. Smith, Milberg and Burke (1996) conceptualized, scientifically crafted and confirmed a four factor solution for consumer concern for information privacy (CFIP) in offline contexts that was comprised of concern about: i) collection of information, ii) unauthorized access to information, iii) improper access to information and iv) errors in information stored by organizations and represented by a fifteen item scale. This conceptualization was previously validated in other off-line contexts (Stewart and Segars, 2002; Rose, 2005) as well. In the studies reviewed here, Lian and Lin (2008) utilized an unaltered version of Smith, Milberg and Burke's (1996) operationalization. Two studies (Bellman et al, 2004; Van Slyke et al, 2006) adapted Smith, Milberg and Burke's scale items to reflect an online context. Though Xu et al (2008) cited Smith, Milberg and Burke (1996) as the source for their privacy concern scale and recognized the multidimensional nature of the construct, the study operationalized the construct with only one item from each of the four dimensions and employed a scale totalling five items.

The work of Smith, Milberg and Burke (1996) was also influential in another three studies as dimensions of CFIP provided the basis of the conceptualization utilized by Dinev and Hart (2004), Malhotra, Kim and Agarwal (2004) and Li, Sarathy and Xu (2010). Malhotra, Kim and Agarwal (2004) developed an Internet User Information Privacy Concern (IUIPC) measure using Smith, Milberg and Burke's (1996) operationalization of consumer concern about information collection and added dimensions justified to represent online privacy. Specifically, IUIPC consisted of the dimensions of information collection, awareness and control. It is possible that Malhotra, Kim and Agarwal (2004) may have confounded the privacy concern construct conceptualization with the inclusion of control, however. Although control was frequently mentioned in philosophical definitions of privacy, Dinev and Hart (2004) clearly showed that control was a construct distinct from privacy concern and no direct correlation between perceived control and privacy concern was found to exist. On the other hand, it must be recognized that the IUIPC conceptualization had subsequently been employed (Buchanan et al, 2007), although the dimensionality of the construct was not analysed.

While Dinev and Hart (2004) cited Smith, Milberg and Burke (1996) and Culnan and Armstrong (1999) as the source for their conceptualization of online privacy concern, the authors clearly conceptualized the dimensionality of privacy concern as consisting of only two dimensions - one’s privacy concern for information finding (PCIF) and one’s privacy concern about information abuse (PCIA). Interestingly, subsequent studies by Dinev and Hart (2006a; 2006b) and Krasnova and Veltri (2010) operationalized privacy concern as PCIA only and the dimension of the construct pertaining to concern about information finding was neglected.

Li, Sarathy and Xu (2010) utilized Malhotra, Kim and Agarwal’s (2004) global information privacy concern (GIPC) scale that was originally attributed to Smith, Milberg and Burke (1996). This was intended to be a succinct, unidimensional representation of privacy concern measured with three items.

Less frequently utilised privacy conceptualisations were employed by Eastlick, Lotz and Warrington (2006) and Castañeda et al (2008). Eastlick, Lotz and Warrington’s (2006) conceptualisation was based upon that of Milne and Boza (1999) and modified to capture consumer concern about specific privacy invasions akin to Prosser’s (1960) defined invasions of disclosure, appropriation and intrusion.

Castañeda et al (2008) adapted conceptualisations originally created for a direct marketing context (Culnan, 1993) and emphasised the philosophical importance of control in privacy via two dimensions – ‘control over collection’ and ‘control over use’. However, just as Malhotra, Kim and Agarwal (2004) may have confounded the privacy construct with the inclusion of control, these authors may have as well.

Three studies (Sheehan and Hoy, 1999; Sheehan and Hoy, 2000; Moscardelli and Divine, 2007) employed a fourteen item situational conceptualisation of privacy concern from a direct marketing context originally presented by Nowak and Phelps (1992). While the core research conducted by Nowak and Phelps provided support for the high incidence of privacy concern and the contextual nature of consumers’ concerns, their exploratory work was not intended to confirm a measure of privacy concern, nor did it do so. Furthermore, Nowak and Phelps (1992) identified their use of the term ‘privacy’ in their measure of concern as a limitation of their study as it had the potential to be poorly interpreted by consumers and use of the term could have even masked individuals’ true concerns (p. 38). It should be noted that subsequent work by Nowak and Phelps (1997) incorporated Prosser’s (1960) legal definition of privacy, yet the authors argued at that time that of Prosser’s four torts of privacy invasion (intrusion, disclosure, false light and appropriation), direct marketers need only concern themselves with appropriation. As the direct marketing applications Nowak and Phelps had been concerned with were primarily one-way communication initiated by the marketer, such an argument is reasonable. However, in the context of immediate, two-way communication afforded by online social networks it is conceivable that all of Prosser’s four privacy invasions are possible and thus, the measures employed by Nowak and Phelps would be insufficient to represent such an environment.

The conceptualisation adopted by Buchanan et al (2007) was unique in a few ways. First, whereas all other studies examined conceptualisations of ‘information’ privacy, this case attempted to represent privacy as a whole including physical privacy and expressive privacy. Second, rather than use previously established scales, the authors generated an original scale of 45 items that were subsequently factor analysed and compared with Malhotra’s IUIPC, ultimately concluding that a general Internet Privacy Concern measuer comprised of 16 items was appropriate.

As expected, various conceptualizations of the construct evidenced in the reviewed literature yielded variation in the resultant factor structure of the construct. Factor solutions for the online consumer privacy concern construct in the selected studies present a range between one and four factors (Table 6). A one-factor solution was commonly produced (Dinev and Hart, 2006a; Dinev and Hart, 2006b; Eastlick, Lotz and Warrington, 2006; Buchanan et al, 2007; Moscardelli and Divine, 2007; Xu et al, 2008; Krasnova and Veltri, 2010; Li, Sarathy and Xu, 2010). Two-factor solutions were reported in three instances (Dinev and Hart, 2004; Casteñeda, Montoso and Luque, 2007; Lian and Lin, 2008). Three-factor (Sheehan and Hoy, 2000; Malhotra, Kim and Agarwal, 2004) and four-factor (Bellman et al, 2004; Van Slyke et al, 2006) solutions were each found in two instances.

Smith et al’s (1996) CFIP construct was shown to consist of the four expected factors when adapted to online contexts (Bellman et al, 2004; Van Slyke et al, 2006), thus validating the instrument and confirming consumers hold concern about information privacy related to collection, unauthorized secondary use, improper access and errors. However, differences did emerge in its presentation as a second order construct with Bellman et al (2004) confirming a reflective relationship and Van Slyke et al (2006) demonstrating a formative relationship. Malhotra, Kim and Agarwal (2004) also confirmed support for this conceptualization in their work, though simultaneously noted the superiority of their own IUIPC at that time.

Where the Smith et al's (1996) operationalization encountered most difficulty was in Lian and Lin's (2008) two-factor solution. Unfortunately, the authors did not discuss the results of their factor solution or provide enough detail to permit further interpretation. Given the cultural relativism argument for privacy (Westin 1967; Moore 2003), it is possible that application of this operationalization to a Taiwanese sample created the differences noted. While there has been support for the measure among an international sample (Bellman et al, 2004) and reliability of the measure among a New Zealand sample situated offline (Rose 2005), the cultures in which the measure was supported may have been more alike the American sample from which it was derived than the Taiwanese sample from which Lian and Lin had been unable to confirm the measure.

The disparities observed among conceptualisations of consumer online information privacy measures were not the only causes of interpretative difficulty from this group of studies. As will be discussed, the concentration of studies using American respondents, the reliance upon student samples and investigators' desires for parsimony each make cross-study comparisons and generalizability of results problematic and lead to some gaps that must be filled in future research.

Geographical Concentration

Most of the examined studies collected data solely from respondents located in the United States (US). An international sample was obtained in one study (Bellman et al, 2004) and Krasnova and Veltri (2010) collected data from respondents in both Germany and the US in order to provide a cross-cultural comparison. Respondents from the United Kingdom (UK) were represented in one study (Buchanan et al, 2007); European responses were captured by Casteñeda, Montoso and Luque (2007); and a Taiwanese perspective was collected in one study (Lian and Lin, 2007). In light of claims that privacy is culturally relative (Westin, 1967; Moore, 2003), theory developed and tested predominantly among samples from one culture present problems in generalizability to other cultural contexts.

Student Dominated Samples

Convenience samples of students were frequently used in the research investigated. Student samples were found exclusively in four studies (Buchanan et al, 2007; Lian and Lin, 2007; Xu et al, 2008; and Li, Sarathy and Xu, 2010). Moscardelli and Divine (2007) used a sample of exclusively high school students as the population of interest was adolescents. While three studies (Dinev and Hart, 2004; 2006a; and Krasnova and Veltri, 2010) did not intend to capture only students, each yielded samples that were dominated by young people. Two studies employed one convenience sample of students (VanSlyke et al, 2006; Casteñeda, Montoso and Luque, 2007) and another sample of ‘consumers’. Only five investigations used exclusively non-student samples (Sheehan and Hoy, 1999, Sheehan and Hoy, 2000; Bellman, 2004; Malhotra, Kim and Agarwal, 2004; Eastlick, Lotz and Warrington, 2006). Details about the sample from Dinev and Hart (2006b) were unclear as the authors indicated soliciting responses from a broad sample but described the age demographic as split between '<30' (59%) and '<30' (41%) (p.15).

To generalize about privacy and privacy concerns from such unrepresentative samples may also be problematic. As noted in a recent review of psychology literature, Henrich, Heine and Norenzayan (2010) revealed that a majority of conclusions drawn about human nature were done so using convenience samples of undergraduate students and young children from Western, Educated, Industrialized, Rich, and Democratic (WEIRD) societies and, rather than being representative of human nature, the samples collected were actually outliers. Further, social networking sites have been argued to have become age-neutral environments that appeal to all types of consumers (Stroud, 2008). Therefore, drawing conclusions about privacy concerns from student dominated samples does not provide a representative picture of the privacy concerns of the online consumer generally, nor the OSN participant specifically.

Parsimony

Another area that presented difficulty in generating comparative insight was authors' interest in parsimony. While the practical limitations of employing extensive scales are appreciated, the complexity of the privacy concern construct warrants a comprehensive treatment. Dinev and Hart's (2004) empirical analysis clearly established a two-factor solution for privacy concern that distinguished privacy concern for information finding (PCIF) as both distinct and related to privacy concern for information abuse (PCIA), yet future studies by these and other researchers (Krasnova and Veltri, 2010) included only PCIA items without justification. Similarly, Xu et al (2008) opted for a parsimonious representation of Smith et al's (1996) CFIP in their investigation of antecedents to privacy concern. While this created a situation where an overall privacy concern was measured, it did not permit examination of interactions of hypothesized antecedents with the various dimensions of the concern construct and prevented further insight into the complex dimensional nature of privacy concern.

Clearly there is, as yet, no one agreed upon definition of privacy. Even when the definition is subject to numerous consistent constraints, many discrepancies in the conceptualisation of consumer online information privacy exist. However, this analysis does reveal one conceptualisation that appears to be emerging as a favoured representation of the construct, particularly in the American context. Smith et al's (1996) representation of CFIP has the three key strengths as revealed herein. Namely, it has been meticulously developed, exhibited a reliable factor structure in external tests and was able to withstand transfer of context from offline to online environments.

3.2 Privacy Paradox

The previous section (Section 3.1) of this literature review provided an overview of the academic understanding of consumer online information privacy concern and provided some insight to the definitions employed in academic investigations. Privacy was also established to be a valuable concept from an academic, philosophical standpoint. The emphasis of Section 3.1, however, was to provide definitional constraints to enable further discussion of consumer privacy in online social networks, but whether consumers are actually concerned about their information privacy has not yet been addressed.

Recall that there are those with vested interests who suggest that ‘privacy is dead’ and consumers must ‘deal with it’ (Scott McNealy *in* Meeks, 2000). Alan Westin, privacy expert and famed author of *Privacy and Freedom* (1967), would wholeheartedly disagree. In 1995, after noting increasing rates of privacy concerns among Americans in various opinion polls, Westin, along with Louis Harris & Associates began surveying the American public to measure privacy concerns (Westin, 2003). Their research identified three segments of the population: i) ‘privacy fundamentalists’ had very high privacy concerns, ii) ‘privacy unconcerned’ were not concerned with privacy issues, and iii) ‘privacy pragmatists’ represented a balance between those two extremes. At the time of the first survey, the privacy pragmatists represented the largest proportion of the population (55%), privacy fundamentalists comprised 25% of the population and privacy unconcerned represented 20% of those surveyed. By 2001, with widespread online communication and rampant data collection by business and government facilitated by technological advancement, privacy pragmatists represented 58% of the population, privacy fundamentalists represented 34% and privacy unconcerned a mere 8%. These results clearly indicated that privacy was not dead in the eyes of consumers. However, an analysis conducted by Kumaraguru and Cranor (2005) did raise questions about the consistency of the privacy index employed in consecutive studies by Westin.

Still, other studies have identified privacy concern as a common sentiment among consumers and reinforce Westin’s claims (i.e. Statistics Canada, 2010). Some statistics revealed that consumers’ information privacy concerns have increased alongside increased digital communication technologies (Westin, 2003) and there are recent public opinion reports indicating consumers were overwhelmingly concerned about their privacy in OSNs (Harris Decima, 2011).

Despite consumers’ self-reported privacy concerns, however, a number of academic studies have observed a counterintuitive phenomenon, where privacy concern claims do not match consumer information disclosure behaviour. While consumers consistently cite feeling concerned about their privacy in OSNs, their privacy attitudes do not prevent participation in OSNs nor sharing copious personal information in these environments. This ‘privacy paradox’ has been defined as “the relationship between individuals’ intentions to disclose personal information and their actual personal information disclosure behaviors” (Norberg, Horne and Horne, 2007).

In two studies, Norberg, Horne and Horne (2007) showed that subjects’ actual information disclosure behaviour significantly exceeded the amount of information subjects reported being willing to disclose. Similarly, in an experimental investigation of consumer privacy attitudes and behaviour in an online shopping context, Spiekerman et al (2001) revealed that given the right circumstances, consumers forgot about their privacy concerns and revealed sensitive personal information without compelling reason. In fact, almost 30% of privacy fundamentalists (those most concerned about privacy and reluctant to disclose personal information despite possible benefit) provided personally identifiable information unnecessarily. Acquisti and Gross (2006) also observed the privacy paradox among participants in OSNs. Given that disclosure of personal information is requisite for participation in OSNs, one might expect privacy concerned individuals to be less likely to join these networks. Further, among privacy concerned individuals who do join, information disclosures would be expected to be minimal. However, Acquisti and Gross (2006) found "that an individual's privacy concerns are only a weak predictor of his membership to the network. Also privacy concerned individuals join the network and reveal great amounts of personal information."

This privacy paradox has drawn increased academic attention of late. We live in an era of near-ubiquitous OSN participation, wherein individuals contribute to these permanent "self-exhibition zones" (Keen, 2012) in an effort to gain a variety of socially derived benefits including relationship maintenance, social surveillance, social discovery, social capital, and social presence. Yet, the very act of participating in OSNs increases privacy vulnerability. And, when asked about how concerned they are about their privacy in these environments, OSN users have overwhelmingly indicated high levels of concern. Thus, the risks associated with these environments are implied to be appreciated.

Clearly, questions abound about how this privacy paradox can be explained. The literature attempting to explain this curiosity is therefore addressed in the next section (Section 3.3).

3.3 Explanations of the Privacy Paradox

The privacy paradox is an intriguing phenomenon that has prompted a number of investigations attempting to explain it. Some of these studies referred to a privacy calculus with which consumers make rational decisions about information disclosure based upon the risks and potential rewards of the information exchange. Other studies, while not referring explicitly to a privacy calculus, have attempted to place privacy concerns in a causal nomological network comprised of constructs that influence information exchange together with privacy concerns.

The purpose of this section of the literature review, then, is to discuss investigations attempting to explain the privacy paradox. This will be done by first discussing the privacy calculus (Section 3.3.1) and the various influences upon information disclosure decisions as derived from privacy calculus literature. From the discussion of those influences suggestions that individual influences and social influences were essential considerations emerged. Thus, Sections 3.3.2 and 3.3.3 present the pertinent individual influences of Communication Privacy Management theory and privacy literacy, respectively. Section 3.3.4 discusses the social influence of trust.

3.3.1 Privacy Calculus

In 2005, Gross and Acquisti observed individuals' paradoxical behaviour with information disclosure on Facebook despite citing privacy concerns. This observation prompted the authors to suggest several hypotheses to explain the phenomenon. Specifically, Gross and Acquisti suggested that the privacy paradox might be explained either by: 1) participants conducting a privacy calculus wherein the benefits of information disclosure exceeding the risks would result in the observed risky information exchange; 2) the privacy settings offered by the OSN provider would permit information disclosure either due to the perceived adequacy of protection offered or oblivion to the privacy settings altogether; 3) peer pressure to disclose information despite the risks or 4) a sense of protection offered by the members of one's network which, at the time of study, included only the campus community, or 5) a combination of these factors. The observation of the privacy paradox and the suggested explanations offered by Gross and Acquisti constitute a seminal piece of literature with respect to information disclosure in OSNs. This work has laid the foundation for numerous scientific investigations and resultant knowledge we now possess about information disclosure decisions in online social networks (OSNs).

Though a seminal work, Gross and Acquisti's (2005) first hypothesis that the privacy paradox might be explained via a privacy calculus was not an entirely new idea; however, its application in online social network settings had not been well established at the time given the novelty of the environment. The notion of 'privacy calculus' is one wherein individuals are willing to disclose personal information in exchange for economic or social benefits (Laufer and Wolfe, 1977) and had been previously discussed in the context of direct marketing (Culnan and Armstrong, 1999). Essentially, this explicative framework is premised on the idea that most people make risk and reward trade-offs with respect to their privacy. As such, research that investigated information disclosure through an economic risk-reward framework is presented first. However, as research into the privacy paradox evolved, findings with respect to social influences, situational influences and individual influences on information disclosure were also brought to light. Therefore, each of these types of influences is also discussed within this literature review.

Economic Influences in the Privacy Calculus

Consistent with Westin's (2003) description of the majority of the American population being 'privacy pragmatists' and Gross and Aquisti's suggestion that some kind of decision calculation is likely employed in information disclosure decisions, a number of academic investigations have attempted to explain individuals' information disclosures from this viewpoint. Although privacy pragmatists have strong feelings about privacy and wish to protect themselves from government and company abuses of their private information, they are also willing to permit access to and use of their information if they understand the reasons for such actions, realize personal benefits and perceive that care has been taken to prevent misuse of their information (Taylor, 2003). Thus, it is logical that privacy pragmatists might undertake a privacy calculus when making decisions to disclose their personal information.

Evidence of a risk-reward economic trade-off was demonstrated quite clearly in two qualitative studies of grocery club cardholders conducted by Sayre and Horne (2000) wherein it was found that retail grocery discounts were sufficient to prompt actual personal information disclosure. Similarly in an online context, Hann, Hui, Lee and Png (2002; 2007) revealed that economic incentives including monetary rewards and future conveniences were able to compensate for less privacy at certain thresholds. And, White (2004) also concluded that consumers engaged in 'disclosure management' (p.48). Specifically, she found that loyal customers were attracted to offers of customized benefits in exchange for personal information until the type of information sought crossed a threshold into a category of embarrassing information. Interestingly, though, respondents would still provide the embarrassing information in White's (2004) study as long as the benefits provided were not customized.

However, persuading consumers to surrender personal information is not quite as simple as requesting information and offering an incentive (i.e. discount, personalisation or convenience). As mentioned above, there are thresholds among incentives at which point the consumer will pragmatically decide disclosure of personal information is not worth the risk (Hann, Hui, Lee and Png, 2002; 2007; White, 2004) – a conclusion additionally supported by Yang and Wang (2009). And, there have been instances in which an incentive was insufficient to prompt information disclosure at all (Ward et al, 2005) and still other assertions that consumers simply do not view their personal information as part of an economic exchange and thus, for whom an economic calculation would never be undertaken (Hoffman et al, 1999).

That economic incentives have been observed to be insufficient criteria to elicit information disclosure from individuals indicates that the relationship is more complex. In fact, as the multidimensional nature of information exchanges had been previously well established (Milne, 1997; Milne and Boza, 1999; Milne and Gordon, 1993), increased complexity in privacy calculi should be expected. The rewards associated with information disclosure may extend well beyond economic incentives as one study from Singapore illustrated (Hui, Tan and Goh, 2006). Hui et al (2006) revealed that both extrinsic and intrinsic benefits were important influences on information disclosure decisions with online companies. Specifically, the authors found that monetary savings, time savings, self-enhancement and social adjustment were the extrinsic benefits influencing the process along with the intrinsic benefits of pleasure, novelty and altruism. Therefore, as we understand the motivations for participation in OSNs to be primarily socially derived and not economically driven, the social influences upon information disclosure decisions are critical to understand.

Social Influences in the Privacy Calculus

Online social networks are inherently social. And, as established in Chapter 2, participation in OSNs is motivated via social capital generally and a variety of specific perceived social benefits. Thus, it is logical to think that there must social influences considered within individuals' information disclosure privacy calculi in these environments. To this end, researchers have variously established that social capital perceptions and tie strength (White, 2004; Stutzman et al, 2012), perceived social contracts with organisations (Culnan, 1995; Culnan and Armstrong, 1999; Milne, 1997; Milne and Gordon, 1993; Malhotra, Kim and Agarwal, 2004; Xu et al, 2008) and power within relationships (Wirtz, Lwin and Williams, 2007) influence information disclosure decisions.

The social capital available to an individual depends in part on the strength of the ties between exchange partners such that individuals in a strong tie relationship tend to interact more frequently and exchange more information, compared to those in a weak tie relationship (Brown and Reingen, 1987). In one study, particularly relevant to the context of OSNs, White (2004) emphasized the role of these ties, or relational bonds. Although White's (2004) research did concentrate on economic incentives as the rewards within a privacy calculus and the relational bond in this context was defined between an individual and an organisation rather than among individuals, the influence of the type of social relationship one held with a company was found to be important in information disclosure decisions. Thus, White (2004) concluded that individuals were more likely to disclose personal information in retail customer relationship management situations and take the 'privacy risk' when they had strong relational bonds with an organisation.

More direct support for the role of social capital in information disclosure decisions was provided by Stutzman et al (2012). In this instance, the authors investigated both bridging (information available from diverse, loose ties) and bonding (social and emotional support available from close ties) social capital and concluded that privacy concerns were indirectly related to social capital. Specifically, these authors determined that privacy concerns have a direct effect on an individuals' information disclosure behaviour on Facebook and that disclosures influenced perceptions of both bridging and bonding social capital. Effectively, this means that information disclosures are made in OSNs in an effort to secure social capital both among close ties and loose ties, but those disclosures are not made blindly for those benefits – privacy concerns influence the information that is disclosed in those environments.

The importance of social influences on information disclosures has also been well established via research employing social contract theory. Under social capital theory, social relations were characterised by implicit exchange contracts, but exchanges with organisations (also known as market exchanges) were noted to require explicit and specific terms (Adler and Kwon, 2002). However, in the context of direct marketing, consumers' exchange of information with companies has long been viewed as an implied social contract (Culnan, 1995; Culnan and Armstrong, 1999; Milne, 1997; Milne and Gordon, 1993) determined by principles of distributive justice, procedural justice and interactional justice (Culnan and Bies, 2003). And, empirical support for the importance of social contracts has been found in research with online entities as well (Malhotra, Kim and Agarwal, 2004; Li, Sarathy and Xu, 2010).

Social contract theory is premised on the notion of bounded moral rationality which states that "individual moral agents lack the information, time, and emotional strength to make perfect judgments" (Donaldson and Dunfee, 1994, p.18). Thus, the implied social contract that occurs between a customer and an organisation any time a consumer provides information to an organisation (Culnan, 1995) serves as a risk-reduction component within one's privacy calculus. Within the social contract is an expectation by the customer that the information they provide to an organisation will be kept safe. Accordingly, research using this theory has claimed that organisations engaged in fair information practices have been able to engender trust from consumers (Culnan and Armstrong, 1999) and thus positively influence consumer information disclosure behaviours (Culnan and Armstrong, 1999; Li, Sarathy and Xu, 2010). And, perceived fair information practices were shown to be more important influences on information disclosure than monetary rewards (Li, Sarathy and Xu 2010).

Although distinct from social contract theory, the power-responsibility equilibrium (PRE) framework developed from social psychology (Emerson 1962) has obvious similarities and has likewise been used to explain individuals' information disclosure decisions (Wirtz, Lwin and Williams, 2007). According to this framework, relationship partners have societal responsibilities based upon their power in the relationship such that the partner with the power has a responsibility to ensure an environment of trust and confidence. Thus, the power-responsibility framework effectively captures the notions of obligation, reciprocity (Coleman, 1988) and trust (Fukuyama, 1995) associated with social capital in hierarchical structural relations (Fukuyama, 1995; Adler and Kwon, 2002).

Wirtz et al (2007) utilized a power-responsibility equilibrium framework to structure their investigation into an implicit privacy calculus wherein the roles played by two power-holding partners in online information exchanges – government and organizations – were evaluated. Accordingly, Wirtz et al (2007) concluded that government regulations reduced consumers' privacy concerns as did organizational policies with respect to one's personal information. And, these privacy concerns mediated privacy behaviours such that privacy concern positively influenced privacy protective behaviours, fabrication of information and withholding information.

Additionally, as social capital theory suggests, social norms have been shown to be influential in information disclosure decisions. Specifically, Lee, Im and Taylor (2008) claimed that reciprocity and sequence were essential considerations in information disclosure decisions. First, under reciprocity, information is disclosed to conversational partners at a level of intimacy matched by that of the partner in order to maintain a level of equity in the exchange. Second, self-disclosure often begets disclosure (Berg and Derlega, 1987), but only if the social norm of sequence is followed. Intimate information disclosure does not precede disclosures of less sensitive or intimate information; instead, disclosures are more likely to occur if the requests for increasingly sensitive disclosures gradually escalate (Altman and Taylor, 1973; Berg and Clark, 1986; Collins and Miller, 1994). Consistent with the claim of social norm importance, Utz and Kramer (2009) showed that perceived norms influenced OSN participants' privacy settings in two investigations of popular European OSNs (Hyves and StudiVZ). Similarly, Moscardelli and Divine (2007) demonstrated that informative peer influence positively influenced privacy concerns in OSNs and Acquisti and Gross (2005) recognized that herding behaviour might be contributing to information disclosure in OSNs despite participants' acknowledged privacy concerns.

Though expressed distinctly, it is clear that each of the social influences discussed in this section is closely related to concepts of social capital and trust. Recall that Chapter 2 described that social capital was defined in certain instances in terms of trust (Coleman, 1988; Fukuyama, 1995; Newton, 1997; Paldam, 2000; Putnam, 2000; Scheufele and Shah, 2000) and that trust was argued to be an acceptable proxy for social capital (Putnam, 2001). Implicit social contracts, by the very nature of being implicit, depend upon trust between parties and organisations employing fair information practices engender trust (Culnan and Armstrong, 1999). The Power-Responsibility Equilibrium theory clearly distinguishes that the creation of trusting environments is the domain of the power stakeholder in a relationship. Further, the social norm of reciprocity is frequently associated with that of trust in game theory investigations (i.e. Berg, Dickhaut and McCabe, 1995; Cox, 2004) and though trust is a distinct social norm (Faulkner, 2010) reciprocity is rarely discussed in its absence. Therefore, to understand the social influences on explanations of the privacy paradox, the commonality among these influences - trust - must be considered in detail. As such, trust and its role in privacy calculus decisions will be explored separately in Section 3.3.4.

Situational Influences in the Privacy Calculus

In addition to economic and social influences, researchers have identified that situational influences and individual factors were influential in information disclosure decisions as well. For example, Poddar et al (2009) conducted a qualitative study using personal interviews among a purposive sample of US Internet users to conceptualise a behaviourist-inspired stimulus-organism-response (S-O-R) framework to explain one's information disclosure decision rules in interactions with online entities. In this theorized explanation, the 'stimulus' was essentially an information request but the situational context of the request was also considered by seeking insight into one's relationship with the requesting entity, the cues offered on a website and the type of information requested. The 'organism' was the individual from whom the information was requested and included consideration of the perceived invasiveness of the request, perceived fair play invoked by the request and the importance of the information exchange. The 'response', then, was characterized in one of three ways: information disclosure, information refusal or exiting the site. While not presented explicitly as a ‘privacy calculus’ typically argued by others, nor measured quantitatively, this article essentially argued that consumers’ decisions to disclose personal information to an online entity are calculated responses based upon evaluations of situational and individual factors. As such, research into the situational influences will be explored in this section, followed by a presentation of individual influences in the following section.

As we saw in Section 3.1, privacy has proved difficult to define and has been noted to be situational and ‘an elastic concept’ (Allen, 1988). In particular, one’s privacy threshold depends on “the information collected, how it is collected, and who collects it” (Cespedes and Smith, 1993, p.13). Among the many situational factors that might be considered in a privacy calculus, sensitivity of the information request appeared to be the prominent area of interest among researchers. As might be expected, consumers in offline context were shown to be more averse to the disclosure of sensitive information, such as financial information, compared with information about their attitudes (Long et al, 1999). Similarly, Phelps et al (2000) found that consumers were most willing to provide demographic and lifestyle data to organisations, but less willing to provide highly sensitive information including financial information and personal identifiers. And, information sensitivity has been shown to influence information disclosures online as well. In an experimental setting using Chinese participants, Yang and Wang (2009) revealed that information sensitivity had significant negative effects on information disclosure. In addition, Xu et al (2008) concluded that the nomological network explaining the antecedents to privacy concern in online environments operated slightly differently based upon the context of information disclosures as each context (healthcare, financial institutions, social networking sites and e-commerce sites) carried with it various implied levels of information sensitivity.

However, it also appeared that the sensitivity of the information request is an insufficient criterion to understand information disclosures online, particularly in OSNs. First, Ward, Bridges and Chitty's (2005) analysis revealed that consumers had no problem providing personally identifiable information online. White (2004) found that while relational bonds influenced the type of information individuals were comfortable disclosing, the most intimate information was not necessarily provided to one's closest ties as the potential loss of face ('face risk') was too great with those ties. And, perhaps most interestingly, Dinev and Hart (2006a) concluded that privacy concerns negatively influenced consumers' intended use of e-services as the level of information disclosure required for use increased *up to a point*; however, the negative relationships between privacy concerns and the most sensitive information disclosures including banking information, social security numbers and medical history were not as strong as those between privacy concern and personal information disclosures required for online shopping transactions.

It is possible that these apparent inconsistencies might be explained based upon the congruity of the information requested with the context of the request. In a retail context, Graeff and Harmon (2002) showed that privacy concerns were reduced when the information requested by a retailer was congruent with the type of information one might expect a retailer to request. Similarly, in their investigation of the power-responsibility equilibrium of information exchanges online, Lwin, Wirtz and Williams (2007) revealed that when the request for highly sensitive information was incongruent with the business context, privacy concern increased dramatically but that incongruent requests were tolerated when information sensitivity was low. Li, Sarathy and Xu (2010) revealed a similar conclusion as well. These authors found that when information collected by an online company had little to moderate relevance to the transaction, intention to disclose information was less than when the request was highly relevant. Curiously however, when the request was for information of little relevance to the exchange and a monetary reward was offered simultaneously, consumers were more averse to disclosing. Clearly, this supports the notion previously expressed that economic calculations are insufficient predictors of information disclosure behaviours, but it also illustrates the complexity of explaining the privacy paradox particularly in light of various situational influences.

These studies highlight that both the sensitivity and congruity of the information request are influential situational influences in privacy calculi. Generally speaking, more sensitive information requests tend to give rise to more intense privacy concerns and lessened desires to disclose information as do incongruous requests for sensitive information. However, it is also important to note that these findings have all been established within direct marketing and online transaction situations - contexts wherein an information request is made of consumers by a company. In OSNs, information is explicitly requested by the service provider (the OSN) in order to create an account, but the majority of the other information disclosures that occur in these environments are *unsolicited,* voluntary self-disclosures made by the participant to members of their network. Thus, consideration of information requests is not directly relevant to understanding the privacy calculus used by OSN participants. Instead, the situational influences affecting information disclosure in OSNs are likely more closely aligned with the participants of one's network and the type and depth of information being shared by those people and thus, are essentially social influences dependent upon trust as discussed in the previous section.

Individual Influences in the Privacy Calculus

There was no shortage of research exploring the influences of individual characteristics within the privacy calculus. Among the studies reporting individual characteristics were findings that personality traits (Hui et al, 2006; Ward, Bridges and Chitty, 2005; Utz and Kramer, 2009), privacy involvement (Long et al, 1999; Rifon, LaRose and Lewis, 2007; Dinev and Hart, 2006c), and individual control (Bellman, 2004; Dinev and Hart, 2004; Dinev and Hart, 2006b; Moscardelli and Divine, 2007; Tow, Dell and Venable, 2010; Van Dyke, Midha and Nemati, 2007; Midha 2012; Xu et al 2008) influenced one's intention to disclose personal information.

Personality Characteristics

As discussed in Chapter 2, self-presentation motivations for OSN participation have been widely acknowledged. Empirical research findings have supported that individuals possessing personality traits consistent with what might be expected of those with self-presentation goals typically disclose more information. For example, Hui et al (2006) determined that the personality characteristics of activity, modesty, friendliness, cheerfulness, adventurousness and sympathy, when matched with appropriate rewards, influenced information disclosure. Ward, Bridges and Chitty (2005) observed a correlation between materialistic consumers and a willingness to provide information. Utz and Kramer (2009) revealed that narcissism was associated with less restrictive privacy settings in one study of users of the European OSN StudiVZ, but did not find the same relationship among Hyves users in a separate study.

Privacy Involvement

In recognition that privacy involvement might be a more apt distinguishing consumer characteristic given the complexity and situational nature of the privacy construct, a few researchers investigated the relationship of privacy involvement in information exchanges. In a seminal work exploring relationship marketing offline, Long et al (1999) revealed that privacy involvement thresholds do exist among customers. Rifon, LaRose and Lewis (2007) demonstrated that privacy involvement influenced privacy concerns which were subsequently connected to privacy-related behaviours[8]. And, though not expressed as ‘privacy involvement’, social awareness, or the “passive involvement and raised interest in social issues” (p.11) is clearly a type of involvement that Dinev and Hart (2006c) revealed capable of reducing privacy concerns.

[8] It must be noted, however, that Rifon, LaRose and Lewis’ (2007) study loses some comparability however due to measurement of the privacy concern construct. In their study, privacy concern was measured with a three item scale within which one item pertained specifically to web site security. As stated in Chapter 2, security falls outside of the definition of privacy employed in this particular work.

Control

Consistent with the discussion of privacy definitions presented in Section 3.1, the concept of control is closely related to privacy. In fact, some authors (i.e., Prosser, 1960; Westin, 1967; Fried, 1970) have incorporated the notion of control into its very definition, thereby equating the two concepts. Other authors, such as Joinson and Paine (2007) recognised that control was a particularly salient component of privacy related to self-disclosure in technological environments. However, Laufer and Wolfe (1977) argued that control likely mediated privacy situations because privacy can exist in the absence of control and vice versa. Accordingly, Dinev and Hart (2004) provided empirical evidence that control was indeed a separate construct in the complex nomological network of which privacy concern is a part. Similarly, Xu et al (2008)'s recognised that control was an antecedent to privacy concern and thus distinct.

Indeed, the literature supports that control has a direct effect on consumers' privacy attitudes. First, Phelps et al (2000) found that direct marketing customers desired more control over their personal information. Milne and Boza (1999) reported that perceived control was negatively related to privacy concern and positively related to direct marketing usage. In the context of online information privacy, rather than investigate perceived control, one's *ability* to control has become the emphasis of a number of studies (Smith, Dinev and Xu, 2011). Specifically, one’s Internet literacy (Dinev and Hart, 2006c) or self-efficacy has been shown to be an important influence on privacy concerns.

Internet experience or familiarity is likely insufficient to indicate an ability to control. While Bellman et al (2004) and Dinev and Hart (2004) showed that Internet experience reduced consumer privacy concern, Moscardelli and Divine (2007) established that teens who used the Internet more, and were thus more familiar, had higher privacy concerns, and Ward, Bridges and Chitty (2005) realized no effect of Internet experience on privacy concern. Seemingly, then, Internet experience may not be the best predictor of one’s *ability* to control their personal information. Instead, Internet literacy, “the ability to use an Internet-connected computer and Internet applications to accomplish practical tasks” (Dinev and Hart, 2006c, p.9) was shown to reduce privacy concerns and positively influence one’s intention to transact with a website. Similarly, Van Dyke, Midha and Nemati (2007) and Midha (2012) concluded that privacy empowerment, or “the individual's perception of the extent to which he/she can control the distribution and use of his/her personally identifying information” (p. 198) influenced privacy concerns in the context of online companies. Further, Tow, Dell and Venable (2010) concluded from a qualitative study of Australian Facebook users that one’s ability to use privacy controls influenced information disclosure decisions of OSN users. Finally, Rifon, LaRose and Lewis (2007) established the importance of one’s privacy self-efficacy for identification of web site authenticity and privacy seals in influencing privacy protective behaviours.

Clearly, control is an essential consideration in consumers’ information disclosure decisions online in light of privacy concerns. But, one criticism noted with the studies endeavouring to understand the role of control in relation to information privacy has been that

> "although control is widely understood to play a significant role in relation to issues of privacy and consent, the conceptualisation of control is typically limited. That is, many … studies see control as little more than the fair information processing principles of notice, choice and access coupled with, at best, the ability to opt–in or out of marketing lists." (Whitley, 2009, p.8).

In his conceptual article, Whitley (2009) presented a case for re-imagining control that better reflected both a complete idea of control and advancements in our technological environment by suggesting that control over information exchanged with organisations need continue throughout one's relationship with the firm and include the option of revoking consent.

Though this study does not seek to explore revocation of information collection and use consent from organisations, the notion that we have an incomplete understanding of consumer control mechanisms is central to our research premise. If we consider that information disclosures made in OSNs occur regularly via numerous activities including status updates, comments placed on network members' pages, posting articles and videos, and private email exchanges with network members, conceptualising control as something that occurs at the outset of a relationship is insufficient.

In the context of OSNs, control is exercised by consumers through each initial information disclosure decision made in OSNs. Before every initial disclosure made by an OSN participant in that environment, the user maintains control over what information to share, how much information to share, and with which members of their network to share the information. Thus, how that control is exercised, or what decision making rules are utilised in OSN information disclosure decisions must be understood. To that end, a theoretical framework of conceptualising information disclosure rules is offered in the Section 3.2.2.

However, although a more complete treatment of control may be required, the elements of control already understood cannot be ignored. Thus, in order to exercise control through a rule-based mechanism presumes a level of competency or 'literacy' or 'self-efficacy'. As shown above, literacy and self-efficacy are important components of control known to influence privacy concerns and behaviours. Therefore, consumers' privacy literacy will be discussed in Section 3.3.3.

3.3.2 Communication Privacy Management Theory as Part of the Privacy Calculus

Communication Privacy Management (CPM) theory (Petronio, 2002) is a boundary theory that has gained some recent attention in its application to personal information disclosures in online environments. Essentially, this theory provides a rule-based system for examining the way people make decisions about their information that strikes a balance between disclosure and privacy in the context of relationships. Communication Privacy Management (CPM) theory is based on the idea that individuals erect boundaries around their personal information and either metaphorically open the boundary to permit information disclosure or close the boundary to restrict information flow. Accordingly, decisions to open boundaries and permit transparency or close boundaries to keep information secret fundamentally depend upon individual control in initial disclosures. Thus, control is a critical consideration of CPM theory (Child and Petronio, 2011).

CPM theory emerged from the presumption that individuals' first believe they own and have a desire and a right to control access to their personal information, that all decisions to reveal or conceal personal information result from dialectical reasoning, and that disclosure decisions are taken with consideration of implications to others. There are three rule management processes within CPM theory: boundary rule formation, boundary coordination and boundary turbulence. Petronio (2002) stated that boundary rules are formed based upon five criteria: 1) cost-benefit ratio, 2) context, 3) motivations, 4) gender and 5) culture. Boundary coordination processes refers to the control that individuals exert over their information sharing behaviour. Specifically, individuals' coordination processes involve complex mental calculations to determine the breadth and depth of personal information to share (boundary permeability, BP), with whom to share their personal information (boundary linkages, BP) and who maintains ownership over their information (boundary ownership, BO). Finally, boundary turbulence occurs when boundary coordination fails. The turbulence may be due to a breakdown of the boundary coordination mechanism by the individuals participating in the exchange or from an outside source, such as a privacy breach.

Though research using CPM had once tended to be concentrated in psychology and dealt with interpersonal information disclosures made in familial exchanges and doctor-patient relationships (Petronio, 2002), CPM has recently been applied in situations where online information privacy is known to be at stake. Metzger's (2007) work was instrumental in determining that CPM theory could also be applied in the context of information exchanges with an online company. Using CPM as an organising framework for the research, Metzger (2007) also supported the idea that individuals engaged in various boundary coordination techniques under different conditions. For example, personal information was disclosed or restricted dependent upon the type of privacy assurance provided by an online company, meaning that boundary permeability was coordinated differently depending on the context. Similarly, Xu et al (2011) applied CPM theory to a variety of types of online companies including OSNs, ultimately revealing that the nomological network for privacy concerns differed depending upon the online context observed. This further suggests that CPM boundaries might be coordinated differently in diverse environments.

Still other researchers have indicated the applicability of CPM theory in social media environments. Waters and Akerman (2011), while using CPM as a theoretical framework to guide their analysis of motivations for Facebook participation, were able to conclude that the five criteria of privacy rule development (Petronio, 2002) were evident in Facebook disclosures. And, boundary coordination processes were empirically measured among a sample of bloggers by Child, Pearson and Petronio (2009) yielding a 'blogging privacy management measure' (BPMM) that confirmed the three boundary coordination processes of boundary ownership, boundary linkages and boundary permeability once information had been disclosed and thus co-owned by bloggers and their readers.

3.3.3 Privacy Literacy as Part of the Privacy Calculus

Consumer awareness and knowledge are known to provide decision making control (Ajzen and Driver, 1991; Armitage and Conner, 1999; Awad and Krishnan, 2006; Chartrand, 2005). In the context of privacy, awareness and knowledge may be referred to as ‘privacy literacy’, or “the understanding that consumers have of the information landscape with which they interact and their responsibilities within that landscape” (Langenderfer and Miyazaki, 2009, 383). In OSNs, an information landscape where the burden of privacy protection rests heavily in consumers’ hands (Langenderfer and Miyazaki, 2009; Nehf, 2007), privacy literacy becomes an increasingly critical asset for consumers to exert control over their personal information in order to minimize privacy vulnerability.

Consumer awareness of privacy-related information has been shown to be an important influence on privacy concerns. In their conceptual work, Foxman and Kilcoyne (1993) even suggested that awareness was a passive dimension of information privacy, the contention being that information privacy could only exist when consumers were informed about data collection and were given control over their information. Consistent with that notion, Malhotra, Kim and Agarwal, (2004) included ‘awareness’ as a dimension of their Internet User Information Privacy Concern (IUIPC) measure. However, ‘awareness’ in this instance did not refer to a consumer’s understanding of their privacy environment, but rather to the value they placed upon organisational information transparency. Other authors (i.e. Culnan, 1995; Milne and Boza, 1999; Milne and Culnan, 2004; Lwin et al 2007; Krasnova and Veltri 2010) have treated privacy awareness as a distinct measure of transparency that influenced privacy concerns and subsequent information disclosures. This treatment was consistent with Nowak and Phelps’ (1992) claim that consumers' privacy concerns were 'only reliable and valid to the extent that consumers are knowledgeable and well-informed' (p.30) about which they are concerned and Buchanan et al's (2007) assertion that "awareness of [privacy related] issues may affect people's behaviour in a wide range of contexts" (p.157).

Research focussing on privacy awareness has tended to emphasise the importance of transparency for firms wishing to reduce consumer privacy concerns in order to permit information disclosure. Culnan (1995) revealed that consumers with greater awareness of direct-mail opt-out options had lower privacy concerns. Consistent with social contract theory, Milne and Boza (1999) concluded that privacy concern was reduced when companies were transparent with their information policies and stressed the relational benefits of their information practices. Similarly, Milne and Culnan (2004) found that consumer privacy risks were reduced by reading privacy notices and Xu et al (2011) revealed that the perceived effectiveness of privacy policies reduced privacy concern. Lwin et al (2007) found that privacy policies reduced consumer concern about information requests from online companies when information sensitivity was low but were insufficient when information sensitivity is high. And, in OSNs, Krasnova and Veltri (2010) revealed that information handling transparency was important for reducing Facebook users' concerns.

But, provision of a privacy policy is not enough to suggest consumers possess a comprehensive understanding of the information landscape sufficient to be categorised as privacy literacy. First, possibly because the length and complexity of many online privacy policies requires patience most consumers do not have (Krashinsky and El Akkad, 2010), people do not read them (BusinessWire, 2010;

Lawler, Molluzzo and Doshi, 2012; Winkler, 2001) or fail to read them thoroughly (Office of National Statistics 2011), many people agree to the policy terms without genuinely knowing to what they have consented. To that end, Facebook users have regularly reported poor understanding of that site's privacy policies (Gross and Acquisti, 2005; Govani and Pashley, 2005; Acquisti and Gross, 2006) and erroneous assumptions (Ofcom, 2008) and clear misinterpretations (Turow, Hennessey and Bleakley, 2008) about the scope of privacy policies have been observed.

Further, despite the links between the ability of organisational information transparency to reduce consumer privacy concerns and thus explain the privacy paradox as highlighted above, there are many suggestions that individuals do not know much about information privacy. In 2002, Cavoukian and Hamilton remarked that 'many consumers are in the dark with respect to how some marketers use their data' (p. 207). Almost a decade later, there was a sense that people remain unaware that their behaviour on OSNs could be putting them at risk (Ofcom, 2008; Office of the Privacy Commissioner of Canada, 2011) and, claims of poor privacy literacy continue. Nissenbaum (2010) has stated that individuals are "not fully aware that at certain critical junctures information is being gathered or recorded. Nor do they fully grasp the implications of the information ecology in which they choose to act." (p.105). Further, it appears that we are not aware of the power of technology to integrate the information we share with a variety of online sources. Specifically, as Cohen (2000) remarked, "people are demonstrably bad at assessing the risk of future harms that may flow from the piece-meal, otherwise consensual collection of their private data" (Cohen, 2000 *in* Solove, 2006).

Evidence suggesting privacy literacy is low has been reported in a number of instances. Namely, Milne and Rohm (2000) concluded a general lack of awareness about what types of information was being collected by direct marketers. Graeff and Harmon (2002) revealed that only a small proportion of consumers surveyed could identify the purposes for which data was collected with their grocery loyalty card. And, as recently as 2009, in a study comparing Irish and American respondents, Keaney found that groups presented differences in the privacy protective measures with which they were aware, but the overall conclusion was that consumer education was still required. In online contexts, consumer knowledge about the details of website privacy policies (Acquisti and Grossklags, 2005; Hoofnagle and King, 2008; Turow et al 2005) and technical and legal privacy protections (Acquisti and Grossklags, 2005) was similarly revealed to be low among U.S. respondents. In fact, Hoofnagle et al (2010) concluded that the majority of Americans were 'privacy illiterate'. Though evidence from Canada is limited, one study did report that just three in ten Canadians were aware of a federal institution that helps them with their privacy and protection of their personal information and, most Canadians felt their knowledge of personal privacy rights under the laws protecting personal information was either poor (36%) or neutral (33%) (Harris Decima, 2011). Additionally, most OSN users neglect to make use of available privacy settings (Gjoka et al, 2011; Govani and Pashley, 2005). Even in instances where respondents claimed to understand the privacy policies of Facebook and make use of the privacy settings, researchers speculated that the weak criteria many use to accept 'friends' into their networks (which in turn allows information to be shared beyond one's assumed control) further signified poor privacy knowledge (Debatin et al, 2009).

Thus, if privacy literacy is an influential component in a privacy calculus as has been suggested by evidence of information transparency reducing privacy concerns, poor privacy literacy could be responsible for the observed privacy paradox. For if we are unaware of the landscape (i.e. risks, ways information is used and disseminated by OSN providers to third parties), then how can we effectively control our decisions and employ boundary coordination rules? In instances of poor privacy literacy, information disclosures may occur despite privacy concerns simply because one is unaware of the privacy risks and/or privacy protections of the OSN technological environment. Yet, drawing such a conclusion is not possible as there are, to this author's knowledge, no studies that have attempted to ascertain a comprehensive picture of consumer privacy literacy as a control measure in online information disclosures. (Excepting Dinev and Hart's (2006c) analysis of Internet literacy and social awareness as individual characteristics that indicated more proficiency in exerting control over one's information environment.)

3.3.4 Trust as Part of the Privacy Calculus

The previous discussion pertaining to control, Communication Privacy Management Theory (Section 3.3.2) and privacy literacy (Section 3.3.3) all dealt with explanations of the privacy paradox from the perspective of the individual because information disclosure decisions are ultimately taken by the individual. However, OSN participation is not a solitary activity. As discussed in detail in Chapter 2, participation in OSNs is primarily motivated by social capital and specific perceived social benefits. Further, Section 3.1.2 presented arguments suggesting that social influences were crucial to explaining the privacy paradox in OSNs. Specifically, it was asserted therein that trust repeatedly appeared as an important social influence within the privacy calculus regardless of the theoretical framework (social capital, social exchange theory, power-responsibility equilibrium) used. Thus, the remaining section of this chapter will address the concept of trust and its role in explaining the privacy paradox as identified in privacy literature.

It would be inconceivable to discuss privacy concerns in online social networks without considering the role of trust for many reasons. First, the need for trust arises under conditions of risk and interdependence (Kapoor, 2009; Milne and Boza, 1999). As we know OSN participation creates privacy vulnerabilities (Ellison, Steinfield and Lampe, 2007), therefore, OSN participants require trust to reduce the threats to privacy that result from information sharing (Sandefur and Laumann, 1998).

Trust can open communication boundaries and is critical to consider in social exchanges of any sort. Nahapiet and Ghoshal (1998) suggested that information senders were more open to information disclosure when trust was present. Similarly, McEvily, Perrone and Zaheer (2003) recognised that trust permitted information flows between individuals in an organisation setting. And, given that relational outcomes such as such as loyalty and cooperation (Gabarino and Johnson, 1999; Tax, Brown and Chandrashekaran, 1998) depend on trust (Sirdeshmukh et al, 2002), the relational outcomes expected among OSN users too, likely are dependent upon trust. As Golembiewski & McConkie (1975) so profoundly stated, trust is “the single most important variable that so thoroughly influences interpersonal and group behaviour” (p.131). Therefore, trust is critical to consider in any type of social relationship and appears to be a necessary condition to overcome vulnerability within information exchanges.

Trust also reduces complexity in social systems (Luhman, 1979) by working as a heuristic (McEvily, Perrone and Zaheer, 2003) to reduce ‘cognitive stress’ (McLain and Hackman, 1999). Rather than functioning as utility maximizers, consumers typically participate in exchange relationships without complete information (Bauer, 1960). Therefore, in the absence of important information such as privacy literacy, trust may serve to reduce cognitive stress in disclosure decisions thereby enabling the exchange of information. Particularly, Pan and Zinkhan (2006) discovered that the mere presence of a privacy policy was a sufficient symbol of trust to increase one’s trust in a fictional online retailer.

Further, given that the typical Facebook user has 141 friends (Smith, 2013) a complexity-reduction measure such as trust permits efficient information disclosure decisions. It would be cumbersome for OSN participants to engage in a complex privacy calculus each time an information disclosure decision was contemplated among network connections. As such, trust in other members of the OSN permits participants to exchange personal information without complete information about each member. Additionally, part of the complexity of the OSN as a social system is that some OSN connections may be with close or weak ties with whom one may interact offline, while other connections may function purely online in the absence of any physical connection. This complete spatial and temporal separation between network members (Smith and Barclay, 1997) necessitates a similar reliance on trust to facilitate information disclosure. Further, that there are different types of ties among network connections (Granovetter, 1973; Sandefur and Laumann, 1998) and within OSNs specifically (Ellison, Steinfield and Lampe, 2007; Pfeil, Arjan and Zaphris, 2009) suggests that not all ties will be trusted equally (Putnam, 1995b) in these environments. Thus, special trust, or trust in specific individuals or institutions (Paldam, 2000), serves to reduce complexity of the social system.

The presence of organisations including the OSN provider also increases the complexity of OSN social system.   Indeed, in offline contexts, the importance of organisational trust had been well established as it was argued to affect relationship quality (Moorman, Zaltman and Desphane, 1992; Campbell, 1997), be an essential characteristic predicting future purchase intention (Gabarino and Johnson, 1999), be necessary for a willingness to provide information to a company (Schoenbachler and Gordon, 2002) and be a more important to marketing strategy than reducing privacy concerns when information exchange was involved (Milne and Boza, 1999). But, ONS have additional complexity due to the presence of other organisational 'silent listeners' - the third party advertisers and application operators that are also privy to one's personal information (Stutzman et al, 2012). The presence of organisational others in information exchanges could increase privacy vulnerabilities and, therefore, trust is required to reduce the complexity of the system and limit privacy risk.

In addition, complexity of the system is further increased because of the nature of the business. Services generally have greater perceived risk and fewer objective standards of evaluation by consumers (Zeithaml, 1981) and online services specifically function with spatial and temporal separation as well. Therefore, organisational trust is required in conjunction with interpersonal trust in OSNs to reduce the complexity of the social system. Accordingly, Acquisti and Gross (2006) and Dwyer, Hiltz and Passerini (2007) demonstrated that organisational trust was distinct among OSN providers. Specifically, Acquisti and Gross (2006) determined that Facebook users do indeed trust that OSN provider and trust the members of that OSN more than they trust the members of other OSNs and Dwyer, Hiltz and Passerini (2007) similarly found that Facebook users trusted that site and its members more than MySpace users trusted either their OSN provider or members.

When examined in relation to privacy concern and information disclosure decisions, trust has been recognised as an important influence in the privacy calculus, though its place within the nomological network is not without question. There is a great deal of support in the literature for negative relationships between privacy concern and trust. For instance, Chellapa and Sin (2005) demonstrated a negative correlation, but no causal direction in the relationship between privacy concern and trust. Culnan and Bies (2003) suggested that trust violations through privacy breaches could increase privacy concerns. In many instances trust has been shown to reduce privacy concerns and lead to a greater willingness to provide personal information (Hart and Johnson, 1999; Long et al, 1999; Shoenbachler and Gordon, 2002; Dinev and Hart, 2006c; Kim, 2008; Luo, 2010) or reasoned to outweigh concern to permit information disclosure (Dwyer, Hiltz and Passerini, 2007; Krasnova and Veltri, 2010). But, a number of investigations have demonstrated that privacy concern has a negative impact on trust (Milne and Boza, 1999; Olivero and Lunt, 2004; Liu et al, 2005; Eastlick, Lotz and Warrington, 2006; Midha, 2012) suggesting unclear relationships about which variables are antecedent to which. Still, in other cases, trust did not function as previous literature findings would suggest it ought (Norberg, Horne and Horne, 2007; VanSlyke et al, 2006). Specifically, Norberg, Horne and Horne (2007) were unable to show a significant impact of trust neither upon one's willingness to disclose nor actual disclosure. Van Slyke et al (2006) found a positive relationship between privacy and trust such that privacy concern led to enhanced trust in one certain online retailer (Amazon.com).

3.4 Concluding Remarks

Privacy is a complex construct that is better discussed when constrained by contextual descriptions. Individuals commonly cite privacy concerns about their personal information in online environments, but paradoxically participate in OSNs and share copious and sometimes sensitive or intimate personal information in these environments. This privacy paradox has prompted substantial academic interest into explanations which may be thought of as privacy calculi wherein individuals attempt to strike some balance between the risk and rewards of participation.

Though various investigations have yielded conclusions about economic, situational, social and individual influences within a privacy calculus, the latter two influences emerged as most pertinent to explanations of the privacy paradox in OSNs. Specifically, individual control was found to be an important consideration in the privacy calculus. Individuals are able to exercise control over their privacy by the ways they coordinate the boundaries surrounding their personal information making Communication Privacy Management theory an important consideration in the privacy calculus. Further, consumer control may also be ascertained by knowledge. Thus, privacy literacy appeared to be an equally important consideration within the privacy calculus. Among the social influences, trust was consistently argued to be critical in OSNs and a crucial component of the privacy calculus.

4 Research Aims, Objectives and Conceptual Model

4.1 Overall Research Aims and Objectives

Online social network participation is reaching a state of ubiquity, particularly among individuals in developed nations. Coinciding with the rise of OSN participation there are increasing privacy concerns among the general public. Participation in OSNs is often motivated by social desires including relationship maintenance and other perceived social capital benefits. Achieving those social benefits is predicated upon sharing personal information within the OSN environment, but information sharing in OSNs increases the vulnerability of the OSN participant's privacy. As a result, OSN participation is paradoxical to stated privacy concerns. Thus, the overall research question guiding this project has been, *How can this privacy paradox be explained?*

While some recent research has attempted to explain the consumer privacy paradox exhibited in OSNs as a type of privacy calculus, our understanding of the phenomenon is far from complete particularly in light of the novelty of the environment. Specifically, while the literature has offered numerous explicit and implicit privacy calculus models, there are still influences in the privacy calculus that have not yet been investigated. The primary aim of this research, then, is *to extend the privacy literature by providing additional understanding of information disclosure decisions in OSNs.*

However, the literature review presented in Chapter 3 provided justification that the concept of privacy is complex. Despite consumer privacy concern being an area of long and continued academic interest, the lack of a commonly accepted definition of privacy has resulted in varied conceptualisations and operationalisations of the construct. Thus, a body of disparate knowledge has emerged among which comparability and extension is challenged. With this in mind, this study holds as another aim: *to offer consistency in its extension of the privacy literature*.

Further, throughout the course of the literature review it became obvious that a Canadian perspective on information disclosure decisions was lacking. Many of the theoretical understandings revealed in the literature review were derived from studies of American subjects. And, although some studies presented data collected from outside the US, a comprehensive understanding of Canadian consumers' attitudes about online information privacy was not found.

As context was acknowledged as an important parameter in privacy investigations (i.e. Goodwin, 1991; Xu et al, 2011), the geographic context from which conclusions were drawn may be argued to be important as well. Indeed, assertions of cultural relativism of privacy (Westin, 1967; Moore, 2003) suggest differences in privacy related decisions across cultures. While cultural differences among Canada and the United States are not generally assumed, sociological comparisons including *Fire and Ice* (Adams, 2003) suggest real differences in the cultural values held by each nation. Using thousands of social values surveys conducted in both countries, Adams identified cultural differences on various matters including religion, authority, the family, consumption, and civic life.

Furthermore, the privacy regulatory environment differs substantially between Canada and the United States. Whereas Canada maintains omnibus privacy legislation (*Personal Information and Protection of Electronic Documents Act, PIPEDA*) intended to shield citizens from privacy threats in all exchanges of personal information with businesses, privacy legislation in the U.S. is not universal. Thus, consumer privacy concern and/or information disclosure decisions in OSNs may reasonably differ given different expectations of privacy protection.

The cultural context of privacy generally, the distinctiveness of Canadian and American culture and the different privacy regulatory environments in each country suggest that conclusions drawn about privacy and privacy in OSNs from samples outside Canada may not be generalizable to the Canadian context. Yet, no comprehensive studies investigating the privacy calculus in this country were found, thereby indicating that an investigation of Canadian consumers' online information privacy concerns is warranted. With this in mind, this study holds as another aim: *to offer a Canadian perspective of privacy concerns and related decisions in OSNs*.

As indicated by the first aim of this Project, the literature reviewed in Chapters 2 and 3 pointed to some critical knowledge gaps in addition to specific issues of context and construct operationalization,. These knowledge gaps, which will be detailed in Sections 4.2, Section 4.2.1 and Section 4.2.2, have yielded the specific objectives of the study. Namely, this research is intended:

1. To validate a prominent conceptualization of privacy concern in the context of online social networks
2. To explain personal information disclosure in online social networks using Communication Privacy Management theory
3. To explain the role of privacy literacy in influencing online social network

information disclosure decisions, and

4. To establish the role of trust in consumer information disclosure behaviours in online social networks.

4.2 Theory Development

The literature review presented in Chapters 2 and 3 supported the idea that personal information disclosure decisions undertaken by individuals in online social networks are complex.

Social capital is the benefit of OSN participation as was recognized explicitly (Lampe, Ellison and Steinfield 2006; Ellison, Steinfield and Lampe 2007; Steinfield, Ellison and Lampe 2008; Pfeil, Arjan and Zaphiris 2009; Valenzuela, Park and Kim 2009) and implicitly (i.e. Acquisti and Gross, 2006; Boyd, 2007; Joinson, 2008; Cheung and Lee, 2009; Hoadley et al 2010) in a variety of investigations. All types of social capital – bridging, bonding and maintained (Putnam, 2000; Ellison, Steinfield and Lampe, 2007) – can all be derived through information exchanges (Coleman 1988; Burt 1992; Nahapiet and Ghoshal 1998; Sandefur and Laumann 1998; Adler and Kwon 2002) with social relations of differing levels of connection (Gronovetter, 1973; Putnam, 2000). However, the exchange of personal information makes an individual susceptible to privacy vulnerabilities generally (Sandefur and Laumann, 1998) and within OSNs specifically (Ellison, Steinfield and Lampe, 2007).

Individuals are not blind to the potential of privacy vulnerabilities in OSNs. When polled, people consistently report being concerned about their privacy (i.e.

Westin, 2003; Statistics Canada, 2010), specifically within online environments (i.e. Harris Decima, 2011), and the prevalence of privacy concerns within the American population has even been noted to have increased in parallel with the rise of digital technologies (Westin, 2003). Despite acknowledged privacy concerns, OSN participation and the information sharing that coincides with it continues to grow (Spiekerman et al, 2001), thus creating a condition known as the 'privacy paradox' (Norberg, Horne and Horne, 2007; Acquisti and Gross, 2006).

Efforts to explain the privacy paradox essentially involved some kind of privacy calculus. Chapter 3 provided insight into the numerous influences that may explain the privacy paradox via some kind of privacy calculus. Specifically, Chapter 3 identified that prior research had variously confirmed economic incentives (Sayre and Horne, 2000; Hann, Hui, Lee and Png 2002 and 2007; White, 2004), individual characteristics (Dinev and Hart, 2006c; Rifon, LaRose and Lewis, 2007; Van Dyke, Midha and Nemati, 2007; Tow, Dell and Venable, 2010; and Midha, 2012), social influences (Culnan 1995; Culnan and Armstrong 1999; Milne 1997; Milne and Gordon 1993; Malhotra, Kim and Agarwal, 2004; White 2004; Wirtz, Lwin and Williams 2007; Xu et al 2008; Stutzman et al 2012) and the situational context of information exchange (Long et al, 1999; Phelps et al, 2000; Xu et al, 2008; Yang and Wang, 2009) explained the privacy paradox to some extent. But, consolidating research of the privacy calculus is complicated due to various conceptualisations of privacy and theoretical frameworks that have been used to frame investigations. To overcome some of this difficulty, Smith, Dinev and Xu (2011), recommend that researchers employ an overarching macro model termed APCO (Antecedents - *Privacy Concerns* – Outcomes). As such, research that has empirically investigated the narrowly defined construct of consumer online privacy concerns has been presented in Table 4.1. For each study only the direct antecedents and direct outcomes of privacy concerns have been isolated.

Table 4.1 Empirical Nomological Networks of Privacy Concern

Study	Object of privacy concern	Direct Antecedents (relationship direction)	Direct Outcomes (relationship direction)
Sheehan and Hoy (1999)	Defined B-to-C contact behaviours	n/a	Register for websites (-); Provide incomplete data (+); Notify ISP about unsolicited email (+); Request removal from mailing list (+); Send highly negative messages (+)
Bellman et al (2004)	Online companies	Internet experience (-)	n/a
Dinev and Hart (2004)	Online	Perceived vulnerability (+)	n/a
Metzger (2004)	Online	n/a	Trust for Website (-); prior online disclosure (-)
Malhotra, Kim and Agarwal (2004)	Online companies	n/a	Trusting beliefs (-); Risk beliefs (+)
Milne and Culnan (2004)	Online	n/a	Read privacy notices (+); trust privacy notices (-)
Dinev and Hart (2006b)	Online	Perceived Internet privacy risk (+)	Willingness to provide personal information to transact online (-)
Dinev and Hart (2006c)	Online	Internet literacy (-); Social awareness (+)	Intention to transact online (-)
Eastlick, Lotz and Warrington (2006)	Fictional insurance company	Services e-tailer reputation (-)	Trust in services e-tailer (-); Purchase intent in services e-tailer (-)
Van Slyke et al (2006)	Online companies generally; merchant specific	n/a	Trust (+); Risk perception (+);
Buchanan et al (2007)	Online	n/a	General Caution (+); Technical Protection (+)
Moscardelli and Divine (2007)	Defined B-to-C contact behaviours	Gender (+female); concept-oriented communication style (+); Informative peer influence (+); Frequency of Internet Use (+); Own email address (+)	Provide inaccurate information when registering for web sites (+); Notify ISP about unsolicited emails (+); Request removal from email lists (+); Flaming entities sending unsolicited email (+)
Wirtz, Lwin and Williams (2007)	Familiar website	Perceived privacy policy coverage (-); attitudes toward regulation (-)	Fabricate (+); Protect (+); Withhold(+)
Lian and Lin (2008)	Organization	n/a	Attitudes toward online shopping for tangible products (-)
Xu et al (2008)	Websites (described by	Privacy intrusion (+); privacy risk (+); privacy	n/a

	category)	control (-)	
Yang and Wang (2009)	Online	n/a	Information disclosure (-); Protection intention (+)
Joinson et al (2010)	Online	n/a	Nondisclosure (+)
Xu et al (2011)	Websites (described by category)	Privacy risk (+); privacy control (-); disposition to value privacy (+)	n/a
Krasnova, Veltri and Günther (2012)	Online social networks	n/a	Self-disclosure (-) for German respondents
Lin and Liu (2012)	Online social networks	n/a	Information disclosure (-); OSN use intensity (+)
Midha (2012)	Familiar Online Retailer	Privacy empowerment (-)	Trust (-)

As shown in Table 4.1., privacy risk, perceived vulnerability and privacy intrusions have been established as antecedents that positively influenced privacy concern (Dinev and Hart, 2004; Dinev and Hart, 2006b; Xu et al, 2008; Xu et al, 2011). Privacy control (Xu et al, 2008; Xu et al, 2011) and the similar construct of privacy empowerment (Midha, 2012) were shown to decrease privacy concerns, although Dinev and Hart (2004) did not find a significant relationship between perceived control and privacy concern. Research demonstrated mixed results with respect to the influence of Internet experience as well. While Bellman et al (2004) and Dinev and Hart (2006c) respectively revealed that Internet experience and Internet literacy had a negative impact on privacy concerns, Moscardelli and Divine (2007) showed that Internet experience was positively related to privacy concern. Thus, *the first knowledge gap identified in this Project stems from the mixed results of control and experience found within the privacy calculus literature*.

Outcomes of privacy concern have tended to be described as behavioural in nature. Specifically, privacy concerns have been shown to have a negative impact upon information disclosure or willingness to disclose (Sheehan and Hoy, 1999;

Dinev and Hart, 2006b; Yang and Wang, 2009; Krasnova, Veltri and Günther 2012; Lin and Liu, 2012) and a negative impact on intentions to transact (Dinev and Hart, 2006c; Eastlink, Lotz and Warrington, 2006; Lian and Lin, 2008). Privacy concerns had a positive impact on privacy protecting intentions and behaviours (Buchanan et al, 2007; Wirtz, Lwin and Williams, 2007; Yang and Wang, 2009) including fabricating or providing incomplete information (Sheehan and Hoy, 1999; Moscardelli and Divine, 2007; Wirtz, Lwin and Williams, 2007), reading privacy policies (Milne and Culnan, 2004), requesting removal from mailing lists (Sheehan and Hoy, 1999; Moscardelli and Divine, 2007) and withholding information (Wirtz, Lwin and Williams, 2007; Joinson et al, 2010).

Clearly, there are a number of actions in which individuals concerned about their privacy might engage. Essentially, research into the consequent behaviours of privacy concern has identified that reduced information disclosure, intentions to disclose less information, or taking privacy protective action commonly occurred. There are two important observations that were drawn from these conclusions. First, these privacy concern outcomes essentially represented another dimension of individual control by identifying ways in which an individual exercises decision control. And, second, none of these conclusions actually measure paradoxical behavior in that each privacy concern outcome is consistent with actions that would be expected when privacy concern are present. This second observation is consistent with Rifon, LaRose and Lewis'(2007) assertion that a privacy paradox does not exist but does not serve to explain the phenomenon that others claim to have observed (Acquisti and Gross, 2006; Norberg, Horne and Horne, 2007). Thus, *the lack of* *emphasis placed upon paradoxical outcomes in the prior literature has been established as the second literature gap in this Project.*

Besides behavioural outcomes, trust was an attitudinal variable commonly cited as an outcome of privacy concern (Metzger, 2004; Malhotra, Kim and Agarwal, 2004; Milne and Culnan, 2004; Eastlick, Lotz and Warrington, 2006; VanSlyke et al, 2006; Midha, 2012). In all but one of the studies identified in Table 4.1, privacy concern had a negative impact on trust (Metzger, 2004; Malhotra, Kim and Agarwal, 2004; Milne and Culnan, 2004; Eastlick, Lotz and Warrington, 2006; Midha, 2012). In the exception, Van Slyke et al (2006) found that privacy concern had a positive impact on trust. However, that conclusion was reached with respect to a familiar online merchant (Amazon.com) which prompted suggestions that perhaps the pre-existing trust in the retailer was influencing the outcome.

This research suggests that trust is likely to be instrumental in overcoming privacy concerns and thus permit information exchange. However, the relationship between trust and privacy concern is not as simple as might be suggested by the relationships in Table 4.1. In addition to the direct effects between privacy concern and trust noted therein, some researchers (i.e. Dwyer, Hiltz and Passerini, 2007) have treated trust and privacy concern independently while other researchers have suggested a ‘symbiotic relationship’ between the constructs (Joinson et al, 2010). Chellapa and Sin (2005) have demonstrated a negative correlation, but no causal direction, in the relationship between privacy concern and trust. Joinson et al (2010) revealed a slight moderating effect between privacy concern and trust on non-disclosure behaviour but concluded that situational trust did not mediate the relationship between privacy concern and non-disclosure. Further, Lin and Liu

(2012) revealed a similar moderating effect of trust on both information disclosure and OSN use and suggested that trust was more dominant in influencing both dependent variables. And, Norberg, Horne and Horne (2007) failed to show a significant impact of trust upon one's willingness to disclose or actual disclosure. These additional findings suggest that *a more conclusive understanding of how trust operates in the privacy calculus of OSN users is required and thus serves as the third literature gap identified in this Project*.

4.2.1 Gaining and Maintaining Control

Control is central to many definitions of privacy (Westin, 1967; Fried, 1970; Parker, 1974; Altman, 1975 and Stone et al; 1983) and control over personal information has been granted special intention in discussions of the construct (Westin, 1967; Fried, 1970; Parent, 1983; Stone et al, 1983) particularly in light of the variety of 'architectural' harms that digital information technologies present (Solove, 2006). While some authors conceptualised control as a dimension of privacy (Sheehan and Hoy, 1999; Malhotra, Kim and Agarwal, 2004), others established that it was a unique construct (Dinev and Hart, 2004). Indeed, among works treating control as a distinct concept, privacy empowerment and perceived control had been shown to be a direct antecedent to privacy concern (Xu et al, 2008; Xu et al, 2011; Midha, 2012).

However, it has been suggested that control, as it relates to privacy, has not received adequate conceptual development (Whitley, 2009). Much of the literature investigating control in privacy calculations has typically treated control as something that exists primarily at the outset of a relationship with a firm. However, information disclosure decisions within OSNs are both *on-going* and *interpersonal*, thus treatment of control in the extant literature has failed to provide a picture of control that is representative of the nature of exchanges in these environments. Furthermore, attempts at assessing the role of control in information disclosure decisions has focused on an individual's *perceived* control but measurement of consumers' *actual control* and understanding of *how it is exercised* in information disclosure decisions in OSNs is lacking within the literature. Therefore, this project proposes that privacy literacy is an appropriate conceptualisation for exploring one way in which control is gained and Communication Privacy Management is an appropriate conceptualisation for understanding how control is maintained.

Privacy Literacy

We are afforded decision-making control based upon the knowledge we possess (Ajzen and Driver, 1991; Armitage and Conner, 1999; Awad and Krishnan, 2006; Chartrand, 2005). Consumer knowledge is comprised of both what one thinks they know about something - subjective knowledge (SK) - and what one actually knows about something - objective knowledge (OK) (Alhabeeb, 2007; Brucks, 1985; Park and Lessig, 1981; Spreng, Divine and Page, 1990; Sujan, 1985). In the context of privacy, that knowledge may be referred to as 'privacy literacy', or "the understanding that consumers have of the information landscape with which they interact and their responsibilities within that landscape" (Langenderfer and Miyazaki, 2009, p. 383). While several authors have documented the importance of privacy awareness in influencing information disclosure decisions (Nowak and Phelps, 1992;

Foxman and Kilcoyne, 1993; Malhotra, Kim and Agarwal, 2004), a complete picture of privacy literacy and its influence on OSN disclosures was not found in the literature.

One way that privacy literacy may be achieved is through experience with the information landscape. Studies that have specifically investigated 'Internet experience' and 'Internet literacy' in the privacy calculus (Bellman et al, 2004; Dinev and Hart, 2006c; Moscardelli and Divine, 2007) carry the implication that experience is a proxy for knowledge; but, although experience may contribute to knowledge, it does not guarantee that knowledge has been acquired. Similarly, studies that have investigated 'privacy self-efficacy' (Rifon, LaRose and Lewis, 2007; Tow, Dell and Venable, 2010) have intended to establish that one's ability to operate privacy controls implies a level of privacy literacy. While this may be the case, studies utilising self-efficacy measures have tended to rely on individual self-reports rather than investigating actual efficacy. In another study, Dinev and Hart (2006c) concluded that social awareness, or passive involvement with social issues, was associated with greater privacy concerns. Implied with this finding is that general awareness of social and political issues suggests greater knowledge of the Internet landscape. However, like self-efficacy measures, the social awareness measure relied upon respondent self-assessment. As such, none of these measures reflect what one objectively knows about privacy. Instead, these measures may be thought as being indicative of one's subjective knowledge, or what one thinks they know about privacy in technological environments.

Still, other authors (i.e. Culnan, 1995; Milne and Boza, 1999; Milne and Culnan, 2004; Lwin et al 2007; Krasnova and Veltri 2010) have treated privacy awareness as organisational privacy policy transparency based upon the understanding that fair information practices will reduce privacy concern and influence information disclosures. However, the mere presence of a policy does not indicate that a consumer has read the policy (Milne and Culnan, 2004) nor does the reading of a privacy policy indicate an understanding of its contents (Gross and Acquisti, 2005; Govani and Pashley, 2005; Acquisti and Gross, 2006; Turow, Hennessey and Bleakley, 2008). It is possible that one who knows to look for a privacy policy on a website or within an OSN might attribute that tactical knowledge to the possession of privacy knowledge and therefore might score more highly on a self-assessed subjective privacy knowledge measure, and by this logic, privacy policy provision would be an indicator of subjective knowledge at best. Although, it is also possible that this type of transparency may be viewed by an individual as a symbol of trust (Pan and Zinkhan, 2006) and, therefore, not indicative of privacy literacy at all.

Thus, to appreciate consumer control in OSNs, a comprehensive examination of privacy literacy via both subjective and objective knowledge measures is required.

Communication Privacy Management

In the presence of privacy concern, individuals can and do exercise control over their personal information via (non)disclosure decisions and privacy protective behaviours, typically expressed as intentions (Sheehan and Hoy, 1999; Dinev and

Hart, 2006b; Yang and Wang, 2009; Krasnova, Veltri and Günther 2012; Lin and Liu, 2012; Dinev and Hart, 2006c; Eastlink, Lotz and Warrington, 2006; Lian and Lin, 2008; Buchanan et al, 2007; Wirtz, Lwin and Williams, 2007; Yang and Wang, 2009). Many of these observations have been derived from the context of business-to-consumer (B2C) interactions and have often examined only behavioural intentions at the outset of the relationship with the organisation.

There is a B2C disclosure element to information sharing within OSNs due to the presence of the OSN provider organisation and third party advertisers and application providers, aka silent listeners (Stutzman et al, 2012). OSNs are unique information sharing environments in that in addition to the known businesses and personal social connections privy to any personal information disclosed, there also exists an 'invisible audience' (Boyd, 2007) of others such as friends-of-friends or the general public who may view certain information shared. However, given that OSN participation is motivated by social capital (Lampe, Ellison and Steinfield, 2006; Ellison, Steinfield and Lampe, 2007; Steinfield, Ellison and Lampe, 2008; Pfeil, Arjan and Zaphiris, 2009; Valenzuela, Park and Kim, 2009), most of the information disclosed in those environments is intended for an audience of social relations rather than business. In addition, rather than being viewed as one-time information disclosures, information provided with OSNs is shared for relationship maintenance purposes (Acquisti and Gross, 2006; Boyd, 2007; Lee et al, 2008; Livingstone, 2008; Subrahmanyam et al, 2008; Young, 2009; Hoadley et al, 2010) which suggests a long term orientation. Further, a critical expectation with social capital is reciprocation (Newton, 1997; Putnam, 2000; Valenzuela, Park and Kim, 2009). Thus, rather than being a one-sided provision of information, information exchange is anticipated.

Therefore, understanding the intricacies of interpersonal information disclosures in the context of privacy concerns is essential.

Communication Privacy Management (CPM) theory was developed with interpersonal information exchange in mind (Petronio, 2002). Recall that CPM theory states that individuals form privacy rules and coordinate the metaphorical boundaries they have erected around their personal information through boundary ownership processes (BO), boundary linkages processes (BL) and boundary permeability processes (BP). Boundary coordination represents an important dimension of control, essentially representing how one exercises their control over information disclosures. Thus, consideration of this theory for OSN information disclosures will contribute to further understanding control processes criticized for being underdeveloped in the privacy literature (Whitley, 2009).

From the literature review presented in Chapter 3, we know that CPM theory assumes that individuals form privacy rules based upon culture, gender, motivations, context and risk:benefit ratio (Petronio, 2002) and that each of the rule foundations was evident in Facebook disclosures (Waters and Akerman, 2011). Furthermore, we have witnessed evidence that each of the theorised boundary coordination processes (BO, BL, and BP) could be empirically detected among a sample of bloggers (Child et al, 2009). Finally, it was even suggested that the privacy paradox may be explained by Communication Privacy Management (CPM) theory as an organising framework (Metzger, 2007; Xu et al, 2011). Although, given the nascent literature in this area, our understanding of CPM as it applies to OSNs is limited.

One unknown about CPM in OSNs is the mechanism by which boundaries are coordinated as it has never been tested. In recognition of the contextual nature of privacy, the unique information exchange environment of OSNs and the presumption that context determines CPM rules, the context of investigation will likely influence boundary coordination. So, while there has been one study that has tested boundary coordination empirically in a context similar to OSNs (blogging), motivations for blogging (i.e. self-presentation) would presumably differ from those for OSN participation (i.e. relationship maintenance, social capital, etc) so that generalising conclusions from one context to the next is not possible. And, unlike unmediated environments wherein communication boundaries and audiences are structurally defined, the mediated environment of OSNs comprised of persistent, replicable, searchable information and invisible audience (Boyd, 2007) creates a truly unique environment with complicated communication boundaries.

4.2.2 Trust in Various Relationship Partners

The literature review suggested that the third gap in knowledge that should be explored in the privacy calculus was the role of trust. Privacy calculus research has concluded that trust can directly reduce privacy concern (Metzger, 2004; Malhotra, Kim and Agarwal, 2004; Milne and Culnan, 2004; Eastlick, Lotz and Warrington, 2006; VanSlyke et al, 2006; Midha, 2012) or function as a moderating concept in disclosure decisions (Joinson et al, 2010; Lin and Liu, 2012) and social capital research has specified the centrality of trust to social capital (Putnam, 1995, 2000; Fukuyama, 1995; Paldam, 2000; and Scheufele and Shah, 2000). However, very little research has linked notions of trust to social capital. Because social capital is an important perceived benefit of OSN participation (Lampe, Ellison and Steinfield, 2006; Ellison, Steinfield and Lampe, 2007; Steinfield, Ellison and Lampe, 2008; Pfeil, Arjan and Zaphiris, 2009; Valenzuela, Park and Kim, 2009) and trust has been argued to be an adequate proxy of social capital (Putnam, 2001), there is support for the integration of these ideas in investigations of the privacy calculus in OSNs.

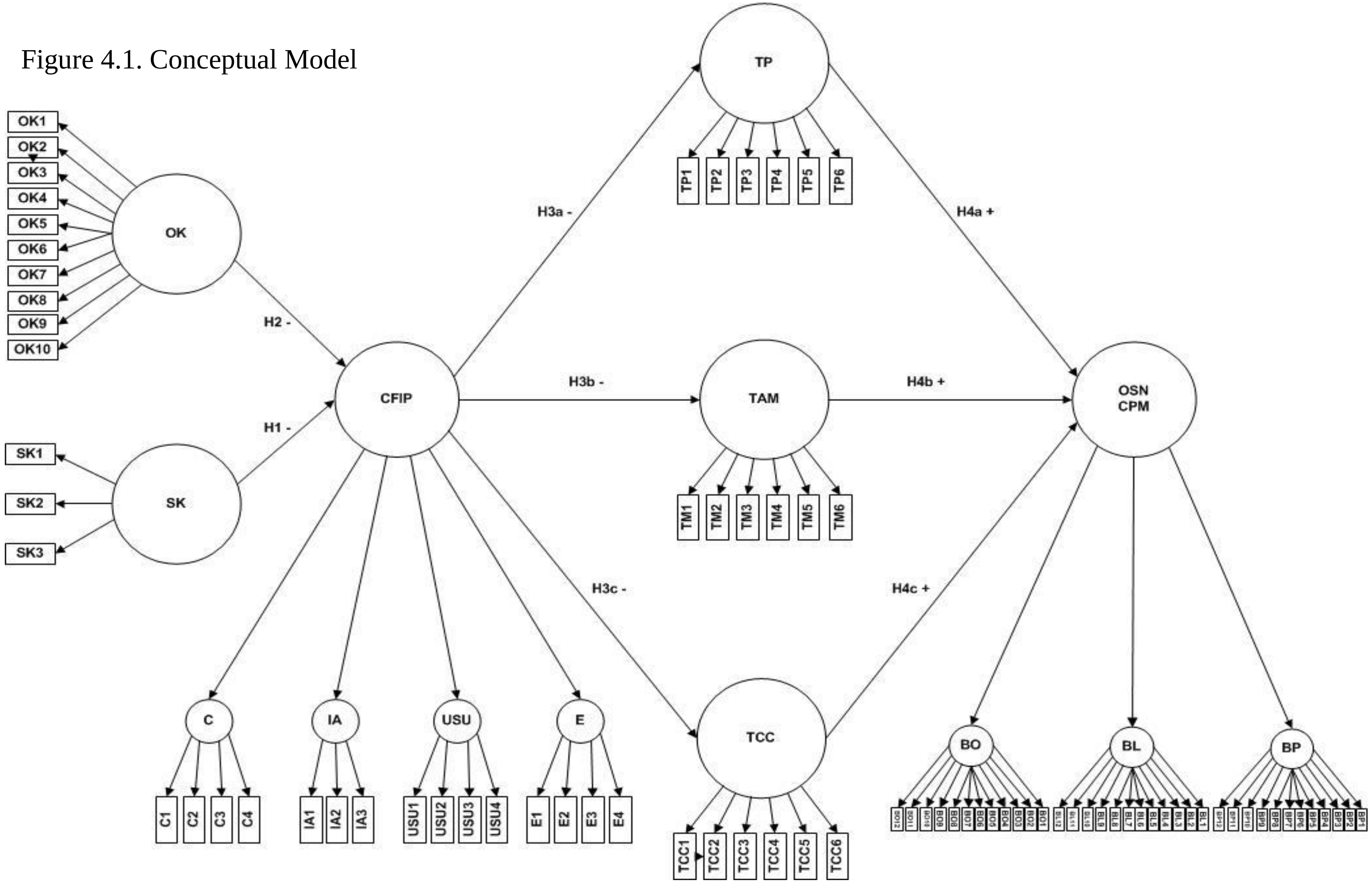
As has been discussed, OSNs have complex communication structures where information disclosures are made to known others (i.e. friends), invisible audiences (i.e. friends-of-friends) and organisational parties (i.e. the OSN provider and third party organisations). Consequently, the various types of interpersonal social capital (Valenzuela, Park and Kim, 2009) - bridging social capital (among weak ties), bonding social capital (among close ties) (Lampe, Ellison and Stutzman, 2006) and maintained social capital (Ellison et al, 2007) - were each observed among OSNs users. Considering that the different types of social capital are distinguished based upon the type of relationship in question and that interpersonal social capital was defined as ‘trust among individuals’ (Valenzuela et al, 2009), it stands to reason that different levels of trust likely exist among different kinds of interpersonal relationships. Indeed, the concept of ‘special trust’ suggests trust does depend upon the relational partner (Putnam 1995b).

Trust is not just an interpersonal construct, though. Much of the privacy calculus research was concentrated upon information exchanges with an organisation, thus, organisational trust tended to be the type of trust examined. In OSNs, trust was observed to depend specifically upon the OSN provider (Acquisti and Gross, 2006; Dwyer, Hiltz and Passerini, 2007), suggesting that trust in the provider would influence information disclosure decisions. Interpersonal trust has been distinguished from organisational trust in privacy calculus literature (Dwyer, Hiltz and Passerini, 2007; Krasnova and Veltri, 2010) as well. However, empirical research that endeavoured to distinguish various types of interpersonal trust and assess its impact on information exchanges in OSNs was not found. Thus, research into the privacy calculus should certainly include trust, but measures of trust should reflect the different kinds of trust that exist between the OSN participant and the range of relational partners in the environment.

4.3 Conceptual Model

The conceptual model is presented in Figure 4.1. This model presents a grounded nomological explanation as to how OSN participants manage their own privacy in light of privacy concerns that accompany participation in such environments. Although there are other antecedents and outcomes of privacy concern, their links have been reasonably well established in the literature (i.e. risk, willingness to transact). As the intent of this Project was to investigate likely relationships in the privacy concern nomological network that had not been well established, only those constructs are modelled and tested.

Figure 4.1. Conceptual Model



4.3.1 Antecedents

As shown in Figure 4.1, privacy literacy was thought to influence privacy concern. Specifically, concern for information privacy (CFIP) was thought to be negatively influenced by one's privacy literacy, represented by objective knowledge (OK) and subjective knowledge (SK). This is consistent with assertions that Internet experience reduced one's privacy concern (Bellman et al, 2004; Dinev and Hart, 2006c). The suggestion is that the more one understands the information landscape within which they operate, the less they will be concerned about their privacy therein. As such, it was expected that individuals confident in their knowledge of privacy related information feel a level of comfort capable of reducing concerns. Therefore, it was hypothesised that:

> H1: *Subjective knowledge (SK) about privacy will influence OSN behaviour by reducing one's concern for information privacy (CFIP).*

Though one may have high subjective knowledge (SK) about privacy, they need not have high objective knowledge (OK) of the same. In fact, while SK and OK have been shown to be related to varying degrees in consumer behaviour studies (Ellen, 1994; Carlson et al, 2007; Moorman et al, 2004; Park, Mothersbaugh and Feick, 1994), it had also been concluded that they were distinct constructs that impact consumer behaviour differently (Brucks, 1985; Park Mothersbaugh and Feick, 1994) and as such, should be treated separately. Similarly, within the privacy literature there have been suggestions that OSN users may be overconfident in their privacy knowledge and/or privacy protecting capabilities (Boyd, 2007; Debatin et al, 2009;

Livingstone, 2008; Youn, 2009), though few explicit investigations exist (excepting Acquisti and Grossklags, 2005; Acquisti and Gross, 2006). In the absence of empirical investigations of the relationship between objective privacy knowledge and privacy concerns, it was rationalised that an individual who is actually privacy literate (i.e. knows about privacy issues, the protections that exist and/or the extent of protections offered) should have lower concern for information privacy. Thus, it was hypothesised that:

> H2: *Objective Knowledge (OK) about privacy will influence OSN behaviour by reducing one's concern for information privacy CFIP.*

4.3.2 Outcomes

Privacy concerns were expected to influence communication boundary coordination processes such that individuals will engage in more rigid boundary coordination in the presence of privacy concerns, in effect exercising more control over their environment to prevent privacy risks. Specifically, those that perceive greater concern for information privacy will hold boundary ownership (BO) more tightly, have fewer boundary linkages (BL) and less boundary permeability (BP). But, trust was thought to be able to overcome or lessen privacy concerns; therefore, trust in all of one's relational partners in OSNs will permit boundary opening and less rigid CPM.

Trust in three key OSN relationship partners –close ties, weak ties, and the service provider – were therefore hypothesised to function as mediating constructs between privacy concern and OSN behaviours. And, as trust and privacy concern have been shown to have a negative relationship (i.e. Joinson et al, 2010) and trust can open communication boundaries (Nahapiet and Ghoshal, 1998; McEvily, Perrone and Zaheer, 2003) the following hypotheses were developed:

H3a: *Concern for information privacy (CFIP) will negatively influence trust in the OSN provider ('trust in provider', TP),*

H3b: *Concern for information privacy (CFIP) will negatively influence trust in all of one's OSN network connections ('trust in all members', TAM),*

H3c: *Concern for information privacy (CFIP) will negatively influence trust in one's close connections within their OSN network ('trust in close connections', TCC),*

H4a: *Trust in the OSN provider (TP) will positively influence OSN CPM,*

H4b: *Trust in all of one's OSN network connections (TAM) will positively influence OSN CPM,* and

H4c: *Trust in one's close connections within their OSN network (TCC) will positively influence OSN CPM.*

5 Methodology

This chapter discusses the research methodology of the Project. It begins with a description of the research philosophy employed and presents the consequent research design. Given the positivist approach to the research, the nomothetic method of survey is subsequently discussed. Data analysis techniques are presented at the conclusion of this chapter.

5.1 Research Philosophy

By now, it should be evident that a number of assumptions about privacy, privacy literacy and trust have been made by this researcher. First, the arguments presented in support of the conceptual model were derived from an extensive literature review. This suggests a core underlying assumption - that conclusions drawn by other researchers are real and true. Specifically, it has been assumed that: 1) individuals do indeed have privacy concerns, 2) individuals' attitudes towards privacy, their knowledge about privacy, their trust in various stakeholders and their information disclosure decisions can be similar and, therefore, grouped, and 3) the aforementioned groupings are "real" and can therefore be measured. These assumptions have shaped the philosophical research paradigm employed herein.

According to Burrell and Morgan (1979), research approaches are classified as either objective or subjective based upon assumptions about the nature of science including ontology, epistemology and human nature. Easterby-Smith et al (2002) similarly argued that at the two philosophical extremes are very different perspectives based upon ontological and epistemological assumptions.

Ontology studies the nature of reality. Purely objectivist ontological approaches, referred to as 'realism' by Burrell and Morgan (1979), are premised on the assumption that reality is external to an individual whereas purely subjectivist ontological approaches, referred to as 'nominalism', assume reality to be the product of individual cognition (Burrell and Morgan, 1979). As mentioned, the underlying assumption in this research is that the phenomena under investigation are externally observable, thus an objectivist ontological approach is indicated.

Epistemology, or the theory of knowledge, seeks to establish what constitutes knowledge and answer the questions of how knowledge is acquired and how we know what we know. A continuum of epistemological approaches has been suggested ranging from the purely objective 'positivist' to the purely subjective 'anti-positivist' (Burrell and Morgan, 1979). The positivist epistemology holds that knowledge acquisition is a cumulative process achieved by the continual addition of new insights either by proving or disproving claims (Popper, 1959; Burrell and Morgan, 1979; Perri 6 and Bellamy, 2012). Positivist epistemologies, then, depend upon the assumption new knowledge is gained through measurements of that external reality. However, although measurement is an essential characteristic, positivism is not synonymous with empiricism (Burrell and Morgan, 1979; Perri 6 and Bellamy, 2012). Positivist epistemologies tend to be characterised by research that requires the investigator remain external to the investigation, utilises hypothetico-deductive approaches, reduces concepts to measurable components and seeks ‘truth’ via identification of regularities and causal relationships between constructs (Easterby-Smith et al, 2002).

Examination of the literature review and conceptual model presented in the previous three chapters indicates that this investigation of consumer information disclosure decisions in online social networks certainly falls at the positivist (Easterby-Smith et al, 2002) or objectivist (Burrell and Morgan, 1979) end of the philosophical continuum. First, the conceptual model represents a cumulative advancement of theory developed primarily based upon hypothetico-deductive measurement of privacy concerns and trust presented by other authors (i.e. Krasnova and Veltri, 2010; Xu et al, 2011). Further, the notion that privacy literacy could be objectively measured was suggested by various studies that measured transparency as an indication of privacy awareness (i.e. Culnan, 1995; Milne and Boza, 1999; Milne and Culnan, 2004; Lwin et al, 2007; Krasnova and Veltri, 2010) and other findings that quantitatively concluded low levels of privacy awareness (i.e. Govani and Pashley, 2005; Gross and Acquisti, 2005; Acquisti and Gross, 2006; Turow, Hennessey and Bleakley, 2008). The boundary coordination component of the Communication Privacy Management theory, though not extensively tested as yet, had been operationalized by Child et al (2009). Finally, the conceptual model was presented as a series of causal relationships formatted as hypotheses.

However, given the metaphysical nature of attitudes such as privacy concern and trust, questions about the extent to which such mental constructs can be verified (Donaldson, 2003) or the extent to which these attitudes could be socially constructed might suggest various research philosophies be employed. While other philosophical approaches could be defended due to the apparent unobservable nature of mental constructs, positivism is not precluded. Because mental constructs can be verified indirectly (Popper, 1959) and the particular attitudes of privacy concern and trust have been treated as such previously (i.e. Smith et al, 1996; Dinev and Hart, 2006; Xu et al, 2011, Krasnova and Veltri, 2010), it was contended that for the purposes of this research, positivism was an appropriate philosophical orientation. Further, as the emphasis of this research is upon how these constructs predict observable things (information disclosure in this case) a positivist research philosophy was additionally fitting (Perri 6 and Bellamy, 2012).

Moreover, Ackroyd (*in* Fleetwood and Ackroyd eds., 2001), maintained that a research paradigm is often selected due to its tradition within an academic discipline. Most consumer research conducted prior to 1985 was empirical and positivist in nature (Deshpande, 1983; Arndt, 1985; and Hirschman, 1985). Indeed, a recent survey of articles published in three ‘top’ marketing journals indicated that the functionalist paradigm, which has also been recognised as a form of positivism, still accounted for the majority of research articles published (Chung and Alagarnatam, 2001). Furthermore, the ‘structurally weighted investigation’, or the more objectivist or positivist approach is acknowledged to be commonplace within marketing (Lowe et al, 2004). Therefore, a positivist approach was justified to be appropriate for this study due to its acceptance within the marketing discipline as well.

5.2 Research Design

Research philosophy directs the appropriate research methods to employ. According to Burrell and Morgan (1979), objectivist approaches yield nomothetic methods, or systematic research protocols. Similarly, Easterby-Smith et al (2002) specified that positivist research progresses through hypotheses and deductions where explanations demonstrate causality. Thus, as the research objectives stated in Section 4.1 identified explanatory inferences be drawn about the influences on information disclosure decisions in OSNs, a causal research design is recommended (Kinnear and Taylor, 1996). Although, 'causal' research designs are typically reserved for experimental research, the types of dependence relationships hypothesised in Section 4.4 of this Project have been theoretically structured as causal, consistent with Hair et al (2010). However, this research is not intended to confirm causality. Instead, as the aims of this research were to explore previously untested dependence relationships, theoretically structured dependence relationships were appropriate. In the absence of experimental conditions or longitudinal data, though, causation cannot be concluded and interpretation of results will require due consideration.

In addition to theoretical or confirmatory causal research designs, positivist methods entail the investigator remaining independent from the research, concepts be operationalized for measurement, statistical analysis be undertaken and large samples be employed (Easterby-Smith et al, 2002). These requirements typically lead an investigator to variable oriented research with between-case analysis (Perri 6 and Bellamy, 2012) accomplished via survey methods (Burrell and Morgan, 1979; Kinnear and Taylor, 1996; Perri 6 and Bellamy, 2012).

A survey method was deemed appropriate for this research given its accordance with positivist research philosophy but also because this Project sought to collect abstract information about individuals' attitudes about privacy, privacy literacy and trust and their subsequent behaviours. Because “we seldom learn much about opinions and attitudes except by surveying” (Cooper and Schindler, 2003, p.319), and questions pertaining to behaviour, attitudes and awareness lend themselves well to survey methods (Malhotra, 2002), a survey method was selected. In addition, cross-sectional surveys are commonplace within the privacy literature (i.e., Culnan, 1993; Culnan and Armstrong, 1999; Garbarino and Johnson, 1999; Long et al, 1999; Milne and Boza, 1999; Phelps et al, 2000; Chellappa and Sin, 2005; Eastlick et al, 2006). Therefore, there was sufficient support for this approach in the context of this investigation.

The appropriate operationalization of constructs is a critical part of the survey method (Easterby-Smith et al, 2002) and recognised as one of the more difficult components of management research (Boyd, Gove and Hitt, 2005; Bryman and Bell, 2003; Echambadi, Campbell and Agarwal, 2006). When it comes to surveying attitudes and the abstract, it is often recommended that sets of questions or attitude scales be used to enhance reliability and validity (Oppenheim, 2001). The first step necessary to develop such sets of questions or multi-item surveys is to conduct a thorough literature review. However, in cases where previously developed measurement scales were questionable, additional scrutiny and refinement of existing scales using qualitative approaches was required. According to Creswell and Plano Clark (2011) embedded mixed methods are appropriate in contexts where instrument development is involved and either qualitative or quantitative approaches are prioritised.

Therefore, consistent with the characteristics of positivist research methods and research design and considerations for instrument development, this Project employed an embedded mixed methods approach with emphasis on the quantitative survey method. The research design depicted in Table 5.1 represents the specific approach undertaken in this Project.

Though presented in earlier sections, a comprehensive literature review and conceptual model development are considered essential steps in the research design of positivist research because of its emphasis upon the cumulative development of knowledge. An extensive literature review allows the researcher to understand what is already known or accepted as truth about the topic and identify gaps in that knowledge base so that theory can be advanced. The survey method was the dominant research method that guided the research design. Within the survey method were a number of stages including survey instrument design, survey pre-test, pilot test and survey administration.   As justified, a mixed methods approach was undertaken wherein developmental qualitative methods were embedded within the survey instrument design and survey pre-test stages of the survey method. Quantitative approaches were comprised of a pilot test and survey administration. Section 5.2.1 discusses the specifics of the mixed methods design employed including the overarching survey design and embedded qualitative approaches.   The specifics of survey instrument design have been presented in Section 5.2.2. Discussion of quantitative methods has been provided in Section 5.2.3. Sample characteristics were identified in Section 5.3. Data collected via the survey method was then prepared and quantitatively analysed. A discussion of data analysis procedures concludes this chapter (Section 5.4).

Table 5.1 Research Design and Outcomes

Approach	Research Stage (Sequential)	Purpose	Method of analysis	Outcomes
	Literature review	Understand OSN motivations; privacy; privacy calculus		- Gaps in knowledge - Research objectives - Conceptual model
Qualitative	Survey instrument design	Operationalize constructs; Avoid incommensurability; obtain ethics approval	- Literature review - Focus group	- Measurement scales for CFIP; OK; SK; TP; TAM; TCC; OSN CPM - Survey preparation - Ethics approval
	Survey pre-test	Test survey software; Assess understanding; readability, completion time	- Focus group	- Survey items modified
Quantitative	Pilot Test	Assess scale reliability; completion time	- Cronbach's α - Descriptive statistics	- Survey finalised
	Survey Administration	Collect data from representative sample of OSN users	- Sample size calculation - Effect size	- Sufficient data for analysis
	Data Preparation	Recode variables; remove missing values	- SPSS v.19	- Data in acceptable format for analysis
	Data Analysis	Test conceptual model	- Descriptive statistics using SPSS 19 v.19 - PLS using SmartPLS 2.0	- Results

5.2.1 Mixed Methods

Mixed method research is an approach that combines qualitative and quantitative forms of inquiry to improve the strength of study (Creswell et al, 2008). Mixed methods approaches can be fixed in advance of the research or emerge as part of the research design as the research process unfolds (Creswell and Plano Clark, 2011) and be classified in a variety of ways (Creswell and Plano Clark, 2011;

Creswell et al, 2003) based upon four critical design decisions. Essentially, the researcher must decide upon how to treat and mix each of the qualitative and quantitative components, or ‘strands’ (Teddlie and Tashakkori, 2009), of the study. Specifically, the researcher must decide i) the level of interaction between qualitative and quantitative research strands, ii) the relative priority of each strand, iii) the timing of the strands and iv) the procedures for mixing the strands (Creswell and Plano Clark, 2011, p. 64).

This Project employed a fixed mixed methods approach with an embedded design variant termed ‘embedded instrument development’ (Creswell and Plano Clark, 2011). In an embedded design, the researcher may add a qualitative strand within a traditional quantitative design or vice versa, but priority is given to one strand over the other. The supplemental strand is added before, during or after the primary strand and direct interaction occurs between the qualitative and quantitative strands of the study via mixing the methods before the final interpretation. The purpose of adding the supplemental strand is to enhance the overall design in some way. Mixed methods research designs have been generally noted to be useful in instrument development (Greene, Caracelli and Brown, 1989; Bryman, 2006) and the embedded instrument development variant of embedded designs, have specifically recognized this purpose (Hilton et al, 2001; Creswell and Plano Clark, 2011). Typically, embedded designs are appropriate when the researcher has the necessary expertise to conduct the prioritized strand in a rigorous way but little prior experience with the supplemental method, when the researcher is comfortable having the research driven by one primary research orientation and/or limited resources prevent placing equal priority on both types of data (Creswell and Plano Clark, 2011).

The specific embedded design employed in this Project emphasized quantitative priority over the qualitative supplemental strand, administered the strands sequentially and required direct interaction of the qualitative and quantitative strands. This design shares similarities with an exploratory sequential design. Specifically, in both designs, qualitative methods can directly interact to inform instrument development and the strands can be employed sequentially (Creswell and Plano Clark, 2011). The difference between these two mixed methods designs, however, was in the priority placed upon quantitative research and the type of mixing that was involved. Exploratory sequential designs may emphasize either qualitative or quantitative strands, but they typically prioritize qualitative approaches (Creswell and Plano Clark, 2011) and are used in instances where new instruments are required to be developed. Further, exploratory sequential designs employ philosophical research approaches consistent with both strands of research (i.e. constructivism for qualitative strands and positivism for quantitative strands). Further, whereas mixing in exploratory sequential designs occurs at the data collection stage with results of the first strand shaping research questions, data collection protocols or instruments, in embedded designs mixing of the supplemental method occurs within the overall design of one of the strands. In embedded designs the supplemental method is conducted specifically to fit the design of the primary strand. In this particular Project, a qualitative strand was embedded within the larger quantitative survey design to develop and refine pre-existing survey instruments, the exact details of which are provided in Section 5.2.1.2.

One major difficulty typically cited about mixed methods approaches is an apparent philosophical conflict. Some have argued that each strand has different epistemological commitments (Smith and Heshusius, 1986) or that qualitative and quantitative research constitute separate paradigms. Others have argued that philosophical issues are not as pronounced because "while epistemological and ontological commitments may be associated with certain research methods … the connections are not deterministic" (Bryman and Bell, 2003, p. 466). Thus, while qualitative and quantitative approaches are frequently associated with certain philosophical paradigms, they need not always be so (Crabtree et al 1993; Wolff, Knodel and Sittitrai, 1993). Furthermore, due to being embedded within a primary research design strand, embedded mixed method designs may suffer from less philosophical conflict as the philosophical assumptions associated with the primary strand are carried through the research (Creswell and Plano Clark, 2011). In the embedded design of this Project, results of the research will be drawn from the quantitative method (survey) with one small component drawn from the qualitative method (focus group). Thus, a consistent positivist paradigm can be held and the argument of paradigm incommensurability minimized (Creswell 1994).

Overarching Quantitative Method - Survey Method

This Project has employed a survey method as the overarching quantitative method in the mixed methods design. Consequently, an online survey comprised of 82 manifest variables measuring the latent constructs of privacy literacy, privacy concern, trust and Communication Privacy Management and 13 respondent descriptor variables was administered to Canadian online social network users using a convenience based snowball sampling technique and survey software purchased from Fluidsurveys.com. Incentivized data collection was conducted over a one month period from November 7, 2011 through December 8, 2011.

Survey methods are capable of capturing data via structured questions with pre-determined responses such as yes/no or scaled answers. Survey methods are advantageous in that they are relatively easy to administer, fixed response questionnaires can eliminate researcher bias and increase reliability of responses, and coding, analysis and interpretation of the data is argued to be simplified (Malhotra, 2002). Unlike other data collection methods, surveys permit the collection of data from large population samples and offer breadth of coverage of a topic. Finally, surveys are recognised to offer economic advantages over other methods and can expand geographic coverage (Cooper and Schindler, 2003). Since this research Project intended to gain a Canadian perspective where respondents are geographically dispersed, this practical advantage of survey was of much interest.

Constructs are typically used in marketing to describe the 'mental abstraction formed by the perception of a phenomenon' (Kinnear and Taylor 1996, p. 230) and serve to simplify complex phenomena, which makes them appropriate for measuring attitudes in marketing studies. However, achieving the cited advantages of the survey method requires precise construct definition and operationalization. In addition, to enable comparison among research and extend knowledge consistent with a positivist orientation, standardised construct operationalization is necessary to avoid difficulties with incommensurabiliy (Kuhn, 1962). However, a noted hindrance within the marketing discipline generally has been the limited use of standardised operationalizations of constructs (Kinnear and Taylor, 1996). The specific problem with unstandardized privacy concern operationalization was highlighted in the literature review presented in Chapter 2 as well. The importance of consistent construct operationalization has resulted in efforts herein to utilize standardised operationalisations of constructs wherever possible. Thus, many scales employed in this survey were used previously and the process discussed in detail in Section 5.2.2. In instances where existing scales were considered questionable or nonexistent, instrument development was a priority and thus required the use of the embedded qualitative strand via focus groups (see subsection *Embedded Qualitative Methods*).

Survey methods are further distinguished based upon their mode of administration (Malhotra, 2002). Decisions about survey mode require trade-offs to balance efficiency with practicality. For this Project, online surveys were deemed to be the appropriate mode of survey administration because of some of the key advantages with the technique including: cost, high speed of data collection, low social desirability bias among respondents, no interviewer bias and no field force problems (Malhotra, 2002). Although there are recognized disadvantages with the mechanism including limited complexity of questions that can be asked, low sample control, low response rates, and no interviewer control of the environment (Malhotra, 2002), the standardisation and practical considerations of cost and speed were reasoned to be more important in this research. Additionally, as a Canadian perspective was a desired outcome of the research, an online mechanism was the only realistic option to reach such a geographically dispersed audience. Furthermore, as the context of the study was online social networks and the sample comprised solely of online social network users, it was reasoned that respondents would be comfortable providing information via this mechanism.

Forced Answers

The survey instrument was comprised of 95 items – 82 manifest variables indicating seven latent constructs and 13 respondent descriptor items. Asking respondents this many separate questions increased the possibility that one or more questions could be missed. Therefore, it was decided that the survey would be designed to force answers. This means that an answer to each question was required on each page of the online survey before the participant could progress to subsequent pages of the survey. In the event of skipped answers, the software would alert the participant that an answer was missing and prompt the individual to enter the omitted information. Forcing answers prevented instances of missing data so that all completed surveys constituted usable responses. Since forcing answers could also risk respondents abandoning the survey, an option of 'prefer not to answer' was included as a response for demographic questions deemed sensitive in nature.

Compensation

Malhotra (2002) recommended that survey response rates could be improved via incentives. Therefore, an attractive incentive was offered for participation in this survey. Upon completion of the survey, respondents were given the opportunity to enrol in a prize draw for an iPad2. In order to participate in the draw, respondents had to provide their email address. To maintain anonymity of respondents, the email addresses of prize draw participants were recorded via an online survey redirect and were not linked to the data collected.

Online surveys were closed on December 8, 2011 and the prize draw for an iPad2 was made on December 9, 2011 at 9:00 am (AST) in Antigonish, Nova Scotia Canada by Dr. Ken MacAulay (Chartered Accountant) and witnessed by Dr. Mary Oxner (Chartered Accountant). The winner was notified by email and the prize was received by the winner in Sydney, Nova Scotia on Sunday, December 18, 2011.

Ethical Issues

The ethical issues associated with this survey were dealt with in several ways. First, ethics approval was acquired from both the degree granting institution and this researcher's employer institution. Next, screening questions for age were designed to eliminate the risks associated with surveying vulnerable age groups. As mentioned, a 'prefer not to answer' option was provided for survey items of a sensitive in nature. Respondents were guaranteed information collected would be anonymous, remain confidential and be destroyed when no longer needed. In addition, participation consent was explicitly requested of respondents before the survey was administered.

The first page of the online survey disclosed pertinent information about the research including its objectives and conditions of anonymity and confidentiality. Respondents were then required to offer or decline consent by selecting a radio button. If respondents did not wish to consent to participation, they could either explicitly decline via the radio button or simply close the survey.

Also, according to Canada's privacy legislation, data collected for research purposes must be maintained on servers located in Canada. As Fluidsurveys.com maintains servers in this country, data collection through this subscription-based third party software ensured compliance with appropriate legislation.

Embedded Qualitative Methods

Two separate focus groups were embedded in the survey design to facilitate instrument development. Focus groups are a method of collecting qualitative data through a group interview on a topic chosen by the researcher (Morgan, 2006). Focus groups yield greater depth of information compared to survey methods, but do not provide the depth associated with individual interviews. This technique is typically employed when meaning and contextual detail are sought (Stewart and Shamdasani, 1990; Wolff et al, 1993), when breadth of information at the individual level is required (Crabtree et al, 1993), when group discussion is the emphasis (Morgan, 2006) and when the degree of consensus on a topic is of interest (Morgan and Krueger, 1993). The success of focus groups is partially reliant upon the participation of respondents. Among the benefits of group interaction are participant release of inhibitions, a widening range of responses, activation of forgotten details, and efficiency of resource deployment (time and money) (Crabtree et al, 1993; Stewart and Shamdasani, 1990). Thus, small, homogenous groups of participants with mutual interest in the discussion topic are desired (Morgan, 2006). Among the cited weaknesses of focus groups are the inability to generalise from the purposive, convenience recruitment techniques typically employed, the time required to conduct these sessions and less stringent standardization (Morgan, 2006). However, the weaknesses of focus groups have been argued to complement survey research nicely (Wolff, Knodel and Sittitrai, 1993).

Although incorporation of qualitative input might appear to contradict a positivist philosophy, it was maintained that inclusion of insights from focus groups to inform survey design only served to increase the rigour of the scientific process espoused by positivism. Use of focus groups prior to survey design have been recognised as beneficial to the development of survey questions (Wolff, Knodel and Sittitrai, 1993; Fuller et al, 1993; O'Brien, 1993), identified as common practice (Stewart and Shamdasani, 1990), and generally supported as an acceptable research method (Creswell, 1994; Echambadi, Campbell and Agarwal, 2006; Shah and Corley, 2006). Most importantly, Wolff, Knodel and Sittitrai (1993) have argued that qualitative research used to inform survey instruments does indeed complement the rigorous scientific approach by providing "independent verification of original theoretical conceptualization on which an isolated survey research design relies so completely" (p. 120). And, within the privacy literature focus groups have also been employed in mixed method designs. For example, Milne and Boza (1998) conducted focus groups to facilitate the development of privacy attitude surveys and Morgan and Hunt (1994) also adopted a mixed method approach to their study of commitment and trust in a business-to-business context.

As mentioned, most of the measurement scales employed in this Project were derived from existing sources. However, as will be revealed in Section 5.2.2, one of the scales contained some questionable items that required further development. As a result, a focus group comprised of peer experts was called upon to provide insight and suggest modifications to the scale in question. This expert panel was comprised of three Marketing and Information Systems faculty from one undergraduate institution. Individuals were purposively selected for participation in the group due to their expertise in survey development, familiarity with online social networks and convenience factors. Insight from the group was sought via an informal focus group discussion wherein participants were provided with the survey in advance of discussion with the researcher. Suggestions from this group were incorporated as identified in the discussion of each construct operationalization.

A second focus group was conducted as part of the survey pre-test. Survey pre-tests are considered an essential step in research using the survey method as they are used to identify and eliminate potential problems with the survey instrument (Malhotra, 2002). Survey pre-tests ideally involve a small group of respondents similar to the desired sample. Pre-tests “provide critical feedback on the choice or wording of questions” (Wolff, Knodel and Sittitrai, 1993, p.120) and have been offered as a solution to some issues with construct validity (Echambadi, Campbell and Agarwal, 2006) and can also aid the researcher in identifying and minimizing certain satisficing behaviours (Krosnick 1999). However, pre-tests have been criticised for being “inherently conservative, sensitive to design flaws arising from questions included and not from questions omitted” (Wolff, Knodel and Sittitrai, 1993, p.120). Thus, pre-tests were employed after survey instrument design was finalised and conducted with the narrow purpose of assessing issues with survey language, layout, length and comprehension.

5.2.2 Survey Instrument Design

Maintaining a positivist orientation, constructs were operationalized consistent with pre-existing measures. Specifically, the survey instrument was comprised of predominantly pre-existing and validated scales. A focus group of peer experts was employed to aid enhancement of scales. And, to minimize satisficing behaviour of respondents, the survey was laid out to provide the most ease to respondents (Krosnick, 2000). Input from a focus group pre-testing the survey instrument provided important opinions and perceptions about mechanisms to reduce complexity for respondents. To elaborate, details of construct operationalization has been discussed in this section specifying both influences from pre-existing published scales and input derived from embedded focus group techniques.

Construct Operationalization

The following section provides details about the operationalization of all constructs used in this research. All scales, excepting that measuring Objective Knowledge, utilised a 7 point Likert Scale format. In addition, all scales, other than that for Objective Knowledge, were derived from previous research; although, modification of original scales was required in certain instances. Each of the scales utilised have been discussed separately below and tables detailing the development process for each construct have been provided in Appendix A.1 throuh Appendix A.5. A complete version of the survey has also been included in Appendix A.6.

Objective Knowledge (OK) Items

Objective knowledge instruments in other marketing research have tended to assess what respondents know about a topic of interest by presenting objective statements the respondent must judge to be true or false (i.e. Carlson, Bearden and Hardesty, 2007) or multiple choice questions about a topic (i.e. Park, Mothersbaugh and Feick, 1994; Moorman et al, 2004). Such measures of objective knowledge have demonstrated convergent, discriminant and criterion validity (Cole, Gaeth and Singh, 1986). However, while objective knowledge has been empirically measured, in each instance it was assessed the measure was specific to the topic of interest, for example pricing knowledge (Park, Mothersbaugh and Feick, 1994; Carlson, Bearden and Hardesty, 2007) or wine knowledge (Mueller, Francis and Lockshin, 1998). As no such instrument was uncovered pertaining to privacy, it was necessary to create an instrument to measure what respondents accurately knew about privacy.

In Canada, all businesses that collect, use and disseminate personal information are governed by the *Personal Information Protection and Electronic Documents Act* (PIPEDA) which was developed according to the seven guiding principles for protection of personal information recommended by the Organisation for Economic Cooperation and Development (OECD). PIPEDA should be familiar to Canadians as it has been in place since 2001, applies to all personal information exchange interactions with business organizations (including but not limited to

OSNs), and there is some responsibility on the part of the consumer to recognize and report violations to the Office of the Privacy Commissioner of Canada. Although some Canadian provinces maintain their own privacy legislation, PIPEDA still applies to federally regulated industries and in instances where interprovincial or international information exchange occurs with a business. Thus, it was rationalized that knowledge of PIPEDA would be indicative of a basic understanding of information privacy in a Canadian context.

Consequently, the Objective Knowledge scale was constructed from a privacy quiz posted on the website of the Office of the Privacy Commissioner (OPC) of Canada. The original quiz included a series of five questions. The quiz was taken four consecutive times by the researcher to extract 11 unique questions. Questions were subsequently modified into a consistent 'true/false/don't know' answer format. Two original questions were removed and an additional question was created about the constitution of a privacy breach. Material for the newly created question originated from an answer to another question provided by the Office of the Privacy Commission. The final scale consisted of 10 items and is shown in Table 5.2. Appendix A.1 contains the original question and answer offered by the OPC, the modified question as it appeared on the questionnaire prepared for respondents and the correct answer to the quiz question.

Table 5.2 Objective Knowledge Scale

Variable	Final Item Answer Options = True, False, Don't Know	Correct Answer	Source
OK 1	When obtaining consent from individuals, an organization can merely advise an individual of the purposes for which the information will be used.	False	New Question
OK 2	Consent to the collection, use or disclosure of	True	New Question

	personal information should not be a condition for supplying a product or a service, unless the information requested is required to fulfill an explicitly specified and legitimate purpose.		
OK 3	If there is legislated need to record an identity document number, like a driver's license number, the document should always be photocopied.	False	New Question
OK 4	The Personal Information Protection and Electronics Documents Act (PIPEDA) covers the collection, use or disclosure of personal information by organizations in the course of commercial activity.	True	New Question
OK 5	An individual's Social Insurance Number should always be used to identify a customer.	False	New Question
OK 6	An organization, which is subject to PIPEDA, uses overt video surveillance for justified security and crime prevention reasons but does not record any images. Since no images are recorded, compliance with PIPEDA is not an issue.	False	New Question
OK 7	A privacy breach occurs when there is unauthorized access to, or collection, use, or disclosure of personal information.	True	New Question
OK 8	An individual can make a complaint to the Office of the Privacy Commissioner of Canada against an organization subject to PIPEDA if an organization denies them access to their personal information.	True	New Question
OK 9	Under certain circumstances, an organization can disclose their customer's personal information to law enforcement officials without their customer's consent.	True	New Question
OK 10	When recording customer telephone calls, organizations must inform the individual that the call may be recorded but not the purposes for which the information will be used.	False	New Question

Subjective Knowledge (SK) Items

The subjective knowledge construct represented what one thinks they know about a topic, or their confidence in their knowledge about a topic. The Subjective Knowledge scale employed in this Project was modified from Carlson et al (2007) where consumers' subjective knowledge of marketers' pricing tactics was explored. The wording of original items was modified for the new object of subjective knowledge - corporate personal information management - and edited for greater clarity based upon survey pre-test feedback. Though the original survey included two groups of two items set as direct opposites, survey pre-test participants indicated that the repetition was unnecessary and reduced clarity of what was expected by respondents. As such, opposing questions were removed. Appendix A.2 shows the original 5 scale items, those presented in the survey pre-test and the resultant finalized scale of three items. Table 5.3 shows the SK scale as it appeared on the survey.

Table 5.3 Subjective Knowledge Scale

Variable	Final Items 7 Point Likert scale	Source
SK1	Compared to most people you know, how would you rate your knowledge about how organizations collect and manage your personal information?	Carlson et al (2007)
SK2	In general, I am quite knowledgeable about how organizations collect and manage my personal information.	Carlson et al (2007)
SK3	I am quite knowledgeable about how the information I provide in my online social network is collected and managed by companies.	Carlson et al (2007)

Concern for Information Privacy (CFIP) Items

The Concern for Information Privacy (CFIP) scale was taken directly from Smith, Milberg and Burke (1996) where CFIP consisted of four separate dimensions – collection (C) (4 items), improper access (IA) (3 items), unauthorised secondary use (USU) (4 items), and errors (E) (4 items). The only change made to this scale was in the framing statement prior to the scale. As privacy concern had previously been shown to be contextual, and this research has endeavoured to measure one's concern about information privacy in online social networks, it was necessary that respondents answer the question in the specific context of their online social network interactions and not with respect to 'all companies'. Table 5.4 shows the scale organised by dimension, though the scale items were scrambled on the actual survey. Appendix A.3 provides the 15 scale items used in the order in which questions appeared on the survey along with the framing statement mentioned above.

Table 5.4 Concern for Information Privacy Scale

Variable	Final Items 7 Point Likert scale 1=Strongly Disagree; 7=Strongly Agree	Source
C1	It usually bothers me when companies ask me for personal information.	Smith et al (1996)
C2	When companies ask me for personal information, I sometimes think twice before providing it.	Smith et al (1996)
C3	It bothers me to give personal information to so many companies.	Smith et al (1996)
C4	I'm concerned that companies are collecting too much personal information about me.	Smith et al (1996)
IA1	Companies should devote more time and effort to preventing unauthorized access to personal information.	Smith et al (1996)
IA2	Computer databases that contain personal information should be protected from unauthorized access – no matter how much it costs.	Smith et al (1996)
IA3	Companies should take more steps to make sure that unauthorized people cannot access personal information in their computers.	Smith et al (1996)
USU1	Companies should not use personal information for any purpose unless it has been authorized by the individuals who provided the information.	Smith et al (1996)
USU2	When people give personal information to a company for some reason, the company should never use the information for any other reason.	Smith et al (1996)
USU3	Companies should never sell the personal information in their computer databases to other companies.	Smith et al (1996)
USU4	Companies should never share personal information with other companies unless it has been authorized by the individuals who provided the information.	Smith et al (1996)

E1	All the personal information in computer databases should be double-checked for accuracy – no matter how much this costs.	Smith et al (1996)
E2	Companies should take more steps to make sure that the personal information in their files is accurate.	Smith et al (1996)
E3	Companies should have better procedures to correct errors in personal information.	Smith et al (1996)
E4	Companies should devote more time and effort to verifying the accuracy of the personal information in their databases.	Smith et al (1996)

Trust Items

Krasnova et al (2010) provided the basis for all trust scale items. Krasnova et al (2010) investigated individual motivation for disclosing personal information in online social networks (OSN) and in so doing utilized trust scales developed from a few notable works within the trust literature. The research conducted by Krasnova et al (2010) was distinct in its treatment of stakeholder dependent trust and that distinction is carried forward in this Project. Krasnova et al (2010) used separate scales to capture one's trust in online social network providers (TP) and trust in other online social network members.

The two trust scales used by Krasnova et al (2010) were provided to the expert panel in their original form. Feedback indicated that respondents might have different levels of trust amongst different reference groups within their online social network. Consistent with social capital theory that strong ties and weak ties are different (Putnam, 2000) and that both kinds of social capital exist in OSNs (Ellison, Steinfield and Lampe, 2007), the group of peer experts suggested that respondents might have difficulty answering questions relating to all OSN members if they were not also given the opportunity to distinguish their trust in their closest network connections. As such, this research included three trust scales – one to measure ‘trust in all members’ (TAM), one to measure trust in the OSN provider (TP) and a new scale to measure ‘trust in close connections’ (TCC).

As with the original source trust scales, there were six items in each of these scales. The TP and TAM items were presented identically to those in Krasnova et al’s (2010) scales. The new TCC scale was operationalized similarly to the TAM scale with only the object of the trust modified. The original scale and its minor modifications are presented in Appendix A.4. The final scale items for each of these three scales are presented in Tables 5.5, 5.6 and 5.7.

Table 5.5 Trust in Provider Scale

Variable	Final Items 7 Point Likert Scale 1=Strongly Disagree; 7=Strongly Agree	Source
	My online social network company...	
TP1	...is open and receptive to the needs of its members.	Krasnova et al (2010)
TP2	...makes good-faith efforts to address most members concerns.	Krasnova et al (2010)
TP3	...is also interested in the well-being of its members, not just its own.	Krasnova et al (2010)
TP4	...is honest in its dealings with me.	Krasnova et al (2010)
TP5	...keeps its commitments to its members.	Krasnova et al (2010)
TP6	...is trustworthy.	Krasnova et al (2010)

Table 5.6 Trust in All Members Scale

Variable	Final Items 7 Point Likert Scale 1=Strongly Disagree; 7=Strongly Agree	Source
	Generally speaking, all my friends and connections…	
TAM1	...will do their best to help me.	Krasnova et al (2010)
TAM2	...do care about the well-being of others.	Krasnova et al (2010)
TAM3	...are open and receptive to the needs of each other.	Krasnova et al (2010)
TAM4	...are honest in dealing with each other.	Krasnova et al (2010)
TAM5	...keep their promises.	Krasnova et al (2010)

TAM6	...are trustworthy.	Krasnova et al (2010)

Table 5.7 Trust in Close Connections Scale

Variable	Final Items 7 Point Likert Scale 1=Strongly Disagree; 7=Strongly Agree	Source
	The friends and connections that I share the most information with…	
TAM1	...will do their best to help me.	New Question
TAM2	...do care about the well-being of others.	New Question
TAM3	...are open and receptive to the needs of each other.	New Question
TAM4	...are honest in dealing with each other.	New Question
TAM5	...keep their promises.	New Question
TAM6	...are trustworthy.	New Question

Online Social Network Communication Privacy Management (OSN CPM) Items

The Online Social Network Communication Privacy Management scale was developed from a measure established by Child, Pearson and Petronio (2009). Child, Pearson and Petronio (2009) originally created a scale consisting of a total of 33 items intended to measure blogging privacy management according to the three theoretical boundary coordination processes of Boundary Ownership (BO), Boundary Linkages (BL) and Boundary Permeability (BP) of Communication Privacy Management (CPM) theory (Petronio 2002). Exploratory and confirmatory factor analysis conducted by Child, Pearson and Petronio (2009) revealed their Blogging Privacy Management Measure (BPMM) was a second order construct with three dimensions (BO, BL and BP) consisting of 18 items (6 for each dimension).

Child, Pearson and Petronio’s (2009) scale was created and used for the specific case of online bloggers. However, as the nature of information disclosures differs between blogs and OSNs, scale item modification was required to accurately reflect online social network privacy management behaviour. In most cases, this meant that original scale items were revised by replacing the word ‘blog’ with ‘status’.

The application of Child, Pearson and Petronio’s (2009) scale to the new context of OSNs was not the only concern. The reliability of the original scale was questionable because the authors chose to retain items with low factor loadings. In their confirmatory factor analysis (CFA), one manifest variable recorded a factor loading of 0.24, well below the recommended minimum of 0.5 threshold (Hair, Black, Babin, and Anderson, 2010). Similarly, another six loadings were below 0.50. Six items had factor loadings between 0.50 and 0.56 and five items had loadings of 0.60 and above including only one item that exceeded the ideal cut-off of 0.70 (Hair et al, 2010). Subsequent tests by the original authors within the same publication led to confirmation of the second order nature of the construct but the final test also included the retention several manifest items with low factor loadings. Despite these concerns, Child, Pearson and Petronio’s (2009) attempt to operationalize the CPM construct has been the only one of its kind in the literature and while their factor loadings were evaluated based upon thresholds for CFA, true confirmation of the factor structure requires validation in additional studies and contexts (Hair et al, 2010).

Given the number of instances in which items were retained despite poor factor loadings, the novelty of the scale, and the desire of this Project to apply CPM theory in the context of OSNs, modification of original items was required. Further, it was determined that the addition of new items could potentially improve the statistical validity of the constructs. Through a focus group of peer experts, new

BO, BL and BP items were created to reflect common information disclosure behaviours in popular online social networks. The new items were added to the original scale. Thus, the final scale presented to respondents contained a total of 36 items - 12 items for each dimension of OSN CPM. Specifically, the scales of BO, BL and BP retained all of Child, Pearson and Petronio's (2009) 18 items and an additional 18 items were added for this study. The finalized version of each scale dimension appears in Table 5.8. The original items and modifications have been detailed in Appendix A.5 along with the original items published by Child, Pearson and Petronio (2009).

Table 5.8 OSN Communication Privacy Management Scale

	Variable	Final Item 7 Point Likert Scale 1=Strongly Disagree; 7=Strongly Agree	Source
Boundary Ownership	BO1	I have limited the personal information posted on my profile.*	Child et al (2009)
	BO2	I use shorthand (e.g., aliases or limited details) when discussing sensitive information so others have limited access to my personal information.*	Child et al (2009)
	BO3	If I think that information I posted really looks too private, I might delete it.*	Child et al (2009)
	BO4	I am slow to talk about recent events because people might talk.*	Child et al (2009)
	BO5	I don't post about certain topics because I worry who can see it.*	Child et al (2009)
	BO6	Seeing intimate details about someone else makes me feel I should keep their information private.*	Child et al (2009)
	BO7	I never tag friends in photos.*	New Question
	BO8	When I am tagged in a photo I remove it immediately.*	New Question
	BO9	I do not share any of my contact information on my profile.*	New Question
	BO10	My birth date is not visible on my profile(s).*	New Question
	BO11	I would like to put my connections in groups so that different people can see different things.*	New Question
	BO12	I have changed my name to prevent people from finding me.*	New Question
Boundary Linkages	BL1	I have created a detailed profile so that others can link to me with similar interests.	Child et al (2009)
	BL2	I try to let people know my best activities and interests so I can find friends.	Child et al (2009)
	BL3	I allow people with a profile or picture I like to access my profile.	Child et al (2009)
	BL4	I comment on or like things on friends' pages to have others	Child et al

		check out my profile.	(2009)
	BL5	I have my privacy settings set to ‘Everyone’.	Child et al (2009)
	BL6	I like to link to interesting websites to increase traffic on my profile.	Child et al (2009)
	BL7	I use social networking links (like the Facebook ‘like’ button) on other websites.	New Question
	BL8	I support companies and people by ‘liking’ pages or making recommendations.	New Question
	BL9	I accept most friend or connection requests I receive.	New Question
	BL10	I like to add ‘applications’ to improve my experience.	New Question
	BL11	I feel uncomfortable saying no to ‘friend’ requests.	New Question
	BL12	I have a limited profile.*	New Question
Boundary Permeability	BP1	When I face challenges in my personal life, I feel comfortable talking about them.	Child et al (2009)
	BP2	I like my status updates or posts to be long and detailed.	Child et al (2009)
	BP3	I like to discuss work concerns publicly.	Child et al (2009)
	BP4	I often tell intimate, personal things without hesitation.	Child et al (2009)
	BP5	I share information with people whom I don’t know in my day-to-day life.	Child et al (2009)
	BP6	I update my profile frequently.	Child et al (2009)
	BP7	I update my status frequently.	New Question
	BP8	When something positive happens to me, I post about it.	New Question
	BP9	My status updates generally indicate how I am feeling.	New Question
	BP10	I like to provide detailed comments on friends’ pages.	New Question
	BP11	When a friend in my network upsets me, I post about it.	New Question
	BP12	When a business upsets me, I post about it.	New Question

*Reverse Coded

Other Survey Items

In addition to the constructs identified above, screening questions, demographic descriptor items and online social network usage items were also measured by the survey.

The survey was intended to capture the perspective of Canadian online social network users. To ensure respondents met these criteria, the following screening questions were included immediately following participant consent: “In which

Canadian province or territory do you live permanently?" and "Have you ever used an online social network such as Facebook, Twitter, Linked In, MySpace or Google+?". In order to prevent issues associated with surveying certain populations regarded as vulnerable, individuals below the age of majority in Canada (18 years) and the senior population were excluded from this research. To do so, a third screening question pertaining to age was included with the other screening questions.

If a respondent was excluded from the research because of their answer to one of the screening questions, they were directed to an exit page of the survey. Respondents who did not meet the sampling criteria were still offered the opportunity to enter the incentive draw for their time.

A series of eight demographic and descriptive questions appeared at the end of the survey. Respondents were asked to provide information about their gender, education level, income range, first language, racial background, urban versus rural geography and the number of devices used to connect to the Internet. Given the sensitive nature of some of these questions but to avoid respondents providing incomplete participants were given the option of 'Prefer not to answer'.

As the research intended to capture opinions and behaviours with respect to online social networks as a whole and not distinguish between the types of OSN used, it was necessary to capture information about OSN use and site preferences among respondents. Respondents were asked to identify the OSNs they 'currently use', 'no longer use' and have 'never used'. A list of twelve popular OSNs was provided for this purpose. The list was based upon rankings of OSNs provided from online sources (Kazeniak, 2009; Unknown, 2009).

Respondents were also asked to identify which of OSNs on the list they used most frequently. For all questions in the survey pertaining to OSNs, respondents were requested to refer to the OSN they identified as their most frequently used network. For clarity, respondents were not required to recall their answer to the most frequently used OSN question. The respondent's answer to that question was automatically inserted into each relevant question by the survey software.

Finally, respondents were asked to describe their frequency of OSN use last month via a forced answer multiple choice question ranging from 'Not at all' to 'More than once per day'.

Survey Pre-Test

The researcher identified a convenience sample of four research assistants at an undergraduate university to pre-test the survey for technological issues with the survey software and survey content. Participants were approached in person by the researcher and upon agreeing to participate were invited to a Marketing Research Lab on the university campus. Upon arrival, participants were welcomed, seated at computer terminals, provided a brief introduction to the research, the purpose of the session and offered consent forms to indicate their consent to continue. Next, participants introduced themselves to the group. Then, participants were instructed to logon to their computer with their university login credentials and open their email accounts. Participants were then directed to open the email they had just received from the researcher which contained a link to the survey and four questions to consider as they progressed through the instrument. Specifically, participants were asked to think about the following: 1) Is the survey what you were expecting after reading the introduction? 2) Were there any questions that were not clear? 3) Can you suggest any ways in which the survey may be improved? 4) How long did the survey take to complete?

Once participants had completed the survey and all had indicated they were prepared to proceed, discussion of the structured questions was undertaken. Each question was addressed in sequence and answers were probed by the researcher to identify appropriateness of language, issues with wording, layout, questions to be added or removed and survey completion time.

The survey took between 13 and 17 minutes for this group to complete. Despite researcher concerns that the survey might be perceived as being too lengthy and respondent fatigue might set in, none of these four respondents felt the survey took too long.

Participants appreciated the layout of the survey citing that only having a few questions appear on each screen was helpful. This response was probed due to the fact there were three pages with 12 items (BO, BL, and BP scales) and one page with 15 items (CFIP scale) and one page with 18 items (TP, TAM, TCC). Respondents indicated that the use of radio buttons to select responses, maintaining consistency in scale format (left=strongly disagree; right=strongly agree) and scale size (7 points) reduced the amount of perceived effort required. They all agreed that the bar at the top of the screen indicating the percentage of the survey that had been completed made them feel as though they were moving quickly through the process as well. When asked about the idea of breaking the longer pages up into smaller sections, they unanimously agreed it was more important to see the progress bar (% complete) move dramatically at the completion of a page.

One individual in the group suggested that the SK scale created some confusion and when probed, the group concurred, offering the suggestion that two items on the subjective knowledge scale be deleted. This change had been previously identified in the Construct Operationalization section of this paper. No issues with language or readability were identified by the group.

5.2.3 Quantitative Methods

With focus group feedback incorporated into the instrument design, the remainder of the survey method was comprised of quantitative methods. Specifically, a pilot test was conducted first followed by the survey being administered to wider sample of respondents.

Pilot Test

A pilot test of the survey was conducted to assess survey completion times and scale reliability. An email invitation to participate in the online survey was sent to 719 undergraduate business students at a small undergraduate university in Eastern Canada on Wednesday, November 2, 2011. Two subsequent reminder emails were circulated to students until the survey close date of November 6, 2011. Two hundred seventeen (217) students responded to the email invitation by initiating the survey, resulting in a 30% response rate. One hundred fifty-three (153) individuals completed the survey in its entirety, providing an effective response rate of 21% and a survey completion rate of 70%.

On November 7, 2011 the 153 surveys returned from students by that date were analysed to assess potential problems with the survey instrument. The demographic characteristics of respondents were also reviewed; however, due to the convenience sample employed, little diversity among this group was expected.

Survey Completion Time

Respondents took an average of 17.59 minutes to complete the survey. This result was consistent with the survey pre-test feedback which indicated the survey took between 13 to 17 minutes to complete. All respondents were required to answer all questions before moving on to the next set of questions within the survey. As such, those completing the survey in an unreasonably short period of time might have done so by randomly clicking boxes rather than thoroughly reading directions or contemplating answers. In the pilot study, 11 respondents (8%) took less than 7 minutes to complete the survey while 33 respondents (21%) took in excess of 20 minutes to complete the survey. While it remained possible that the shorter completion times represented less reflective responses (a satisficing behaviour), the incidence of rushing did not appear to be common. On the other hand, that almost 21% of respondents spent more than the suggested amount of time with the survey might suggest appropriate attention was paid to the questions. However, this extended completion time did also raise minor concerns that a respondent may fatigue before completing the instrument in full.

Demographic Characteristics of Pilot Test Respondents

Great diversity among the demographic characteristics of pilot test respondents was not anticipated due to the fact that the sample was generated by convenience from a group of students in one program of study at one undergraduate institution. Instead, the demographic characteristics reported here have been provided for information only.

The sample for the pilot test was young with 97% (N=149) between the ages of 18 and 24 which was consistent with the population sampled. Respondents were slightly more female (54%) than male (45%) and an overwhelming majority were Caucasian (92%) and considered English to be their primary language (92%). Facebook was resoundingly the favourite OSN among this group with 91% (N=139) reporting they used that site most frequently over other OSNs. Further, this group was comprised of active OSN users. Almost 89% (N=136) reported using their favourite OSN at least once per day with most (80%, N=122) reporting usage in excess of one time per day.

Scale Reliability

Scale reliability of survey constructs was assessed using Cronbach's α, an accepted measurement of internal consistency of scales. Results are presented in Table 5.9 and the findings subsequently discussed.

Table 5.9 Scale Reliability of Pilot Test (N=153)

Scale Name	Number of Items	Mean	Min	Max	Chronbach's α
Concern for Information Privacy (CFIP)					
• Collection	4	5.505	5.163	5.967	.846
• Unauthorized Secondary Use	4	5.980	5.784	6.111	.890
• Improper Access	3	5.858	5.778	5.902	.910
• Errors	4	5.119	4.706	5.333	.888
Communication Privacy Management					
• Boundary Ownership	12	3.724	1.712	5.608	.498
• Boundary Linkages	12	2.646	1.739	3.699	.796
• Boundary Permeability	12	2.528	1.647	3.673	.876
Privacy Literacy					
• Objective Knowledge	10	1.872	1.556	2.425	.794
• Subjective Knowledge	3	3.939	3.667	4.203	.830
Trust					
• Trust in OSN Provider	6	4.108	3.654	4.386	.900
• Trust in All OSN Members	6	4.124	3.876	4.405	.948
• Trust in OSN Close Connections	6	5.353	5.222	5.529	.948

All the scales that were extracted from existing literature were determined to be internally consistent (Cronbach's α = 0.70) and thus reliable (Hair et al, 2010). CFIP Collection (α = 0.846), CFIP Unauthorised Secondary Use (α = 0.890), CFIP Improper Access (α = 0.910), CFIP Errors (α = 0.888), SK (α = 0.830), TP (α = 0.900), and TAM (α = 0.948) were all well above the minimum threshold of scale reliability. Though the 'trust in close connections' (TCC) scale had not been previously used, Cronbach's α for the measure (α = .948) was among the highest recorded and just at below the threshold (α > .95) where one might be concerned about item redundancy. The Objective Knowledge (OK) scale was created solely for this research thus the scale reliability was of great interest. The test statistic for OK (α = 0.794) also revealed scale reliability.

Because the OSN CPM scales (BO, BL and BP) were not externally validated in the literature and their original form included items with weak factor loadings, and also because six new items were added to each scale, it was unclear whether these scales would exhibit internal consistency. Both Boundary Linkages (α = 0.796) and Boundary Permeability (α = 0.876) produced acceptable internal consistency measures but Boundary Ownership (α = 0.498) was well below the recommended threshold indicating the scale was unreliable.

Comparison of the original scales of 6 items with the modified versions which included 12 items (Table 5.10) indicated that the original Boundary Ownership scale was more reliable (Chronbach's α = 0.521) than the modified version (Chronbach's α = 0.498), but the original scale was still unacceptable in internal consistency. The modified Boundary Linkages scale and the modified Boundary Permeability scales were more reliable (Chronbach's α = 0.796 and Chronbach's α = 0.876, respectively) than the original scales (Chronbach's α = 0.760 and Chronbach's α = 0.777, respectively). Though the enhanced scales improved reliability of the measures slightly, the original scales were determined to be sufficiently reliable on their own.

Table 5.10 Comparison of OSN Communication Privacy Management Original and Modified Scale Reliabilities

	BO Modified Scale	**BO Original Scale**	**BL Modified Scale**	**BL Original Scale**	**BP Modified Scale**	**BP Original Scale**
Number of	12	6	12	6	12	6

Items						
Mean	3.724	4.735	2.696	2.337	2.528	2.367
Min	1.712	3.578	1.739	1.739	1.647	1.712
Max	5.608	5.608	3.699	2.608	3.673	3.261
Chronbach's α	.498	.521	.796	.760	.876	.777

While these results indicated that there may be some issues with the Boundary Ownership measure, the homogeneity of the pilot test sample could not be excluded. Therefore, it was decided that the BO scale would be retained as the full 12 item scale and re-evaluated once all data had been collected. No modifications were made to the survey instrument as a result of the pilot test.

Sampling Technique

Purposive sampling, “a form of non-probability sampling in which decisions concerning the individuals to be included in the sample are taken by the researcher, based upon a variety of criteria which may include specialist knowledge of the research issue, or capacity and willingness to participate in the research” (Oliver, 2006, p.244), was used to collect data for this research. Nonprobability sample designs involve some kind of subjective judgment by the researcher about the selection of units of the population in the sample (Henry, 1990). Convenience samples and snowball samples are two types of nonprobability sampling techniques (Henry, 1990) that have been used in this research.

Convenience samples are those selected based upon their availability for the study while snowball samples are those selected from group members identifying additional members to be included in the sample (Henry, 1990; Bryman, Teevan and Bell, 2009). With the snowball sampling technique, the recommendation process continues like a snowball, or chain letter, such that new recommendations are provided by each respondent (Davidson, 2006). Consistent with these approaches, the sampling design of this study entailed using a convenience sample to reach an initial group of respondents and those respondents contacted other potential respondents directly or provided the contact information of others to be contacted by the researcher.

Nonprobability sampling techniques allow for expedient data collection and efficient use of scarce resources and are also considered appropriate within exploratory research approaches or when there is an inability to identify members of the population (Henry, 1990; Bryman, Teevan and Bell, 2009). Indeed, in situations where sampling frames are absent, non-probability samples are often a reasonable choice (Adams, Khan and Raeside, 2007) and purposive samples “can provide valuable information…in the early stages of an investigation (Lohr, 2010). Each of these criteria were present in this study, thus a case could be realistically made in support of nonprobability sampling techniques.

First, no external funding supported this study, thus limited financial resources were available. Timeliness of data collection was of the essence given the rapidly evolving nature of the OSN environment and the time frames for doctoral study. The objectives of this research were to extend the current privacy calculus literature by testing new relationships and thus, to that extent, the research could be considered exploratory. Finally, but most importantly, the lack of a sampling frame led the design toward a nonprobability sample.

Snowball sampling is particularly appropriate in instances where populations are hard to find or hard to reach. These ‘hard to reach’ populations can include populations where there is no sampling frame or only a very incomplete one (Henry, 1990; Brymen, Teevan and Bell, 2009; Marpsat and Razafindratsima, 2010). There remains no sampling frame of Internet users (Bryman, Teevan and Bell, 2009) much less a sampling frame for online social network users. Accordingly, probability sampling of Internet users was recognised as a difficult undertaking (Bryman, Teevan and Bell, 2009) and the argument can be similarly extended to OSN users. While OSN users have a common behaviour (OSN usage) the lack of a sampling frame constituted OSN users as a hard to reach population appropriate for snowball sampling. Indeed, while there are limitations to virtual sampling strategies, Bryman, Teevan and Bell (2009) have argued that given the scarcity of knowledge about online behaviours, some information is better than none at all (p. 206). Furthermore, cross-sectional surveys using non-probability samples have been recognised to be acceptable for dissertation purposes as results do provide some indication of behaviours and attitudes of a particular group (Brynner, 2006).

However, although nonprobability sampling techniques could be justified, they were not without important limitations that must be considered when interpreting results. Specifically, nonprobability samples have been criticised for the inability to generalise results to the population, the selection bias that is introduced by the researcher and unresolvable questions about the external validity of the results (Henry, 1990). As types of nonprobability samples, both convenience samples and snowball samples suffer from these limitations. However, the selection bias introduced through snowball sampling may result in more homogeneity of the sample as referrals tend to be passed along to individuals similar to the initial respondent (Marpsat and Razafindratsima, 2010). Further, while the overall sample achieved using nonprobability techniques may appear representative of a given population in terms of demographic characteristics, results are still not generalizable to the larger population given the selective judgment imposed in the initial sample (Lohr, 2010). Finally, self-selection bias and nonresponse bias were potential limitations of these sampling techniques, though not specific to nonprobability samples. With probability and nonprobability samples alike, there remains the possibility that nonrespondents differ from respondents and that those that opt to participate in the research might do so because they have something to say about or a particular involvement with the topic (Lohr, 2010).

Sampling Procedure

The convenience samples for this research were identified in four ways. Participants in each of the survey design components of expert panel and survey pre-test focus groups involved purposive convenience selection by the researcher. In the case of the expert panel focus group, specialist knowledge and availability were the selection criteria used whereas ease of access and availability were the criteria employed in the case of the pre-test participants. Second, students in one program of study at the researcher's undergraduate university were used as a convenience sample for pilot testing the survey. Contacts within the researcher's online social networks served as a third convenience sample. Finally, advertisements were purchased on two popular online social networks and one popular search engine as a means of reaching potential respondents through the medium of study.

In the case of survey instrument development it was necessary to recruit the aid of an expert panel to provide insight on scales that did not pre-exist in the literature. The three individuals whose input was sought all had experience with survey development, were familiar users of online social networks and were readily available. Similarly, the research assistants selected to participate in the survey pre-test were selected due to their familiarity with online social networks and their availability. Pilot testing the survey via convenience sampling was justified for accessibility and resource reasons and was consistent with assertions that early stages of research were conducive to convenience sampling (i.e., Lohr, 2010).

Results of the pilot test showed no need to modify the survey further; therefore the survey was re-opened and a subsequent email reminder was distributed to students on November 21, 2011. A total of 39 additional students initiated the survey during this time and 30 completed the questionnaire. The total convenience student sample included 256 individuals who initiated the survey and 183 completed surveys yielding a 36% initial response rate and a 25% effective response rate. As the objective of the pilot test was to assess measurement reliability and not structural relationships and no modification of the survey resulted from the pilot test, the results of the pilot were included with the remainder of the results for analysis of the research model.

Using the convenience snowball method, 475 email invitations were circulated to this researcher's Facebook and LinkedIn contact lists on November 8, 2011. Those contacted were requested to share the survey link among friends and colleagues. A reminder email was circulated to all the researcher's original contacts on November 10, 2011 and Facebook status updates were used as additional reminders. At the close of the survey on December 8, 2011, 777 individuals had initiated the survey and 539 completed questionnaires had been collected (69% completion rate). Response rates for this wave of data collection were impossible to calculate as it is unknown how many individuals were introduced to the survey due to the snowball technique employed.

A series of online advertisements were created and run in conjunction with the convenience snowball sample of researcher contacts to attract additional respondents. Because the sample of interest was online social network users, ads were placed on two such popular sites - Facebook and LinkedIn - and targeted to Canadians between the ages of 18-64. The Facebook advertisement ran from November 11th to 30th, 2011 reaching 310,482 individuals with 816,979 impressions and generated 456 clicks for a click-through rate of 0.06%. One hundred forty-one (141) of the 456 (31%) individuals redirected to the survey began the questionnaire; 73 individuals were both eligible to continue and completed the survey in its entirety yielding a completion rate of 52%. The LinkedIn advertisement ran from November 11th to 22nd, 2011. By November 21, 2011 it had generated 55,183 impressions from which 5 individuals clicked the link. One usable survey was obtained from this contact method. The ad was deemed unsuccessful at generating respondents and was not continued. Reasoning that OSN users are online regularly, an advertisement was also placed with Google and ran from November 14th – 22nd, 2011. This ad generated 109,927 impressions from which 154 individuals clicked the link, yielding a click-through rate of 0.14%. Fifty-six of the 154 (42%) individuals redirected to the survey began the questionnaire; 17 individuals were both eligible to continue and completed the survey in its entirety yielding a completion rate of 30 %.

Keeping with the snowball technique, survey respondents were requested to provide the email addresses of individuals they felt would be interested in completing the survey. As a result, 166 email invitations were collected through this mechanism and were distributed on November 14th. Sixteen of those emails were returned as undeliverable. Initially, twenty individuals receiving the invitation through this mechanism initiated the survey and fifteen respondents completed the survey yielding an overall response rate of 13% and an effective response rate of 10%. A reminder email was sent to these suggested participants and additional four new suggested contacts on November 23, 2011. A further 19 individuals initiated the survey upon being reminded and thirteen of those respondents completed the survey. The response rate for initiated surveys was 25% and 18% for completed surveys. The overall completion rate of this survey was 72%.

5.3 Sample Characteristics

The sample size calculation for this research was determined using accepted rules for partial least squares analysis. The minimum sample size required should be equal to the larger of either: (1) ten times the largest number of formative indicators used to measure one construct, or (2) ten times the largest number of structural paths directed at a particular latent construct in the structural model (Hair, Ringle and Starstedt, 2011). Based upon this rule, the minimum sample size for this study is 30. However, other researchers have suggested that minimum sample sizes of 100 would be required to ensure acceptable fit (Nasser and Wisenbaker, 2003).

Total Sample Size

A total of 883 surveys were initiated. Forty-five surveys were terminated due to ineligibility of respondents based upon one of three screening questions which included age, Canadian residency, and online social network experience and thus excluded. Once ineligible respondents were removed, the total usable sample size was 838. An analysis of missing items was conducted in SPSS v. 19. Although survey responses were forced, there were three cases for which the CFIP IA item 3 answers was missing. Inspection of the survey software code revealed that the forced answer option had not been set correctly for this item, but rather than do a mean replacement of the item, each of these three cases were deleted. The remaining usable sample size was therefore 835.

Sample Demographics and Usage Characteristics

Sample demographics and OSN usage characteristics are presented in Tables 5.11 and 5.12, respectively.

A vast majority (91%) of the study sample used Facebook as their favoured OSN and were heavy OSN users (85%), logging into their accounts at least once a day, with most (70%) claiming to visit their favoured OSN more than once per day. Most respondents connected to the Internet via more than one device (82%), with approximately one quarter (26%) of the sample using four or more devices.

The study sample was more heavily female (64%) and somewhat young (18 – 24 yrs = 32%; 25 – 34 yrs = 21%; 35 – 44 yrs = 26%; 45 – 54 yrs. = 11%; 55 – 64 years = 9%). The majority of respondents were Caucasian (90%) whose first language was English (93%) and the majority of respondents lived in Atlantic Canada (69%). A small proportion of respondents (2%) did not complete high school, 26% reported high school as the highest level of education achieved, 17% completed college, 35% held Bachelor's degrees, 11% held Master's degrees, 3% had doctoral degrees, and 6% declined to provide educational attainment. Total household income under $20,000 was reported by 11% of respondents, 11% reported $20,000 - $39,999, 14% were in the $40,000 - $59,999 range, 13% reported $60,000 - $79,999, 11% were in the range of $80,000 - $99,000, 23% had household incomes above $100,000 and 15% declined to provide this information.

Table 5.11 Demographic Overview of Respondents

	Survey N	Survey %
Gender		
Male	282	33.8
Female	540	63.7
Prefer not to answer	13	1.6
Age		
18-24	273	32.6
25-34	177	21.2
35-44	216	25.9
45-54	95	11.5
55-64	74	8.8
Education		
Did not complete high school	14	1.7
High school or equivalent	220	26.3
College diploma	142	17.1
Bachelor's degree	292	35.0
Master's degree	91	10.9
Doctoral Degree	23	2.7
Other	35	4.2
Prefer not to answer	18	2.1
Income		
Under $20,000	95	11.3
$20,000 - $39,999	94	11.3
$40,000 - $59,999	121	14.4
$60,000 - $79,999	109	13.1

$80,000 - $99,999	96	11.5
$100,000 or more	194	23.2
Prefer not to answer	126	15.2
Canadian Province of Residency		
Atlantic Provinces	575	68.9
Quebec	27	3.2
Ontario	104	12.4
Western Canada	124	14.8
Territories	5	0.6
Geographic Location		
Urban	514	61.6
Rural	321	38.4
Race		
White/Caucasian	755	90.5
Black/African Canadian	10	1.2
Asian	19	2.3
Aboriginal	12	1.4
Indian	4	0.5
Spanish/Hispanic/Latino	4	0.5
Other	12	1.4
Prefer not to answer	19	2.3

Table 5.12 Usage Characteristics

	Survey N	Survey %
Number of Devices Used to Access Internet		
1	151	18.1
2	207	24.7
3	259	30.9
4	121	14.4
More than 4	97	11.8
Preferred Online Social Network		
Facebook	761	91.1
Twitter	43	5.1
Linked In	8	1.0
Google +	21	2.5
Other	2	0.2
Frequency of Online Social Network Usage Last Month		
Not at all	3	0.4
Once	8	1.0
Twice	9	1.1
Once per week	29	3.5
A few times per week	75	8.9
Once per day	129	15.4
More than once per day	582	69.7

Representativeness of Sample

Although the sample was not representative of the Canadian population in terms of regional geographic distribution, gender, or racial distribution, the sample achieved was reasonably representative of the demographic characteristics of online social network users. Consistent with the study sample, Facebook is reportedly used by 90% of all OSN users (Ipsos Reid 2011 Fact Guide). The disproportionate representation of Atlantic Canadian respondents was not thought to be problematic as Atlantic Canadians have been observed to have 'historically been in line with technological trends' (Cosgrove 2012, p.C4). Though the gender distribution of the sample achieved for this study was predominantly female (64%), that result is not unlike the gender distributions observed in online social networks environments (Ipsos Reid, 2009; Dewing, 2010; Madden and Zickuhr, 2011) nor those collected in other online social network research. For example, Cardon et al's (2009) study of online and offline personal connections required collection of data from individuals in eleven societies in which the sample was predominantly female (59%). Likewise, Young's (2011) sample was 76 per cent female. And, no significant differences in OSN use were observed "based on race and ethnicity, household income, education level, or whether the internet user lives in an urban, suburban, or rural environment." (Madden and Zickuhr, 2011, p.3). Thus, the study sample appears to represent the demographics of OSN users quite well.

5.4 Data Analysis Techniques

5.4.1 Data Preparation

To prepare data for analysis certain variables had to be recoded and missing values had to be addressed. Data was prepared using SPSS v. 19.

All twelve items of the Boundary Ownership scale plus one item (item 12) of the Boundary Linkage scale were reverse coded. Thus, responses to these questions were transformed for analysis. The Objective Knowledge scale was the only scale that did not measure items on a 7 point Likert scale. Instead, respondents answered each of the 10 items as either 'True', 'False, or 'Don't Know'. In order to determine how much one actually knew about privacy (OK), these items had to be scored to reflect correct and incorrect answers. As such, answers that were correct (e.g. the respondent selected 'True' when the answer was 'True') were assigned a value of 1. Answers that were deemed incorrect either by virtue of selecting the wrong answer or selecting 'Don't Know' was assigned a value of 0. This meant that the final measures became binary in nature.

As mentioned earlier, only three variables in the study sample had missing data. The three cases associated with the missing data were deleted from analysis.

5.4.2 Reflective versus Formative Constructs

Reflective measures dominate social science research (Hair et al, 2010). By treating a measure as reflective, the researcher is essentially saying that the latent construct causes the indicator variables. Indicator variables of reflective constructs are highly correlated. Formative measures, on the other hand, are based upon the idea that the indicators cause the latent construct. Manifest indicators in formative measures do not have to be correlated and high collinearity among formative items is problematic.

All the constructs in the conceptual model were thought to be reflective constructs. Trust measures and OSN CPM has been treated as such in previous literature. CFIP was alternatively concluded to be a *reflective* second-order construct (Bellman et al, 2004) and a *formative* second-order construct (Van Slyke et al, 2006). This model treated CFIP as a reflective second order construct.

Finally, OK was determined to be a reflective construct using distinguishing characteristics specified by Hair et al (2010). It was reasoned that the sampling of items about *PIPEDA* selected from the Office of the Privacy Commissioner of Canada constitute a representative sample of items about privacy, but not an exhaustive inventory of items, thus the domain of the construct is clearly reflective. Further, it was expected that the indicator items of OK would vary together (be collinear) since all the items are conceptually related.

5.4.3 Data Analysis

The partial least squares (PLS) approach to structural equation modelling (SEM) was used to analyse data using SmartPLS 2.0 (Ringle, Wende, and Will 2005). First developed by Wold (1982), PLS-SEM has become an increasingly popular technique in marketing research (Babin, Hair and Bole, 2008). Both covariance based (CB) SEM and PLS-SEM are techniques used to assess structural models in empirical causal research. CB-SEM is recommended in instances where theory confirmation is the goal whereas PLS-SEM is recommended for research that tends to be more exploratory and seeks theory extension (Hair et al, 2011). Whereas CB-SEM techniques provide measures of goodness-of-fit of a proposed structural model, PLS-SEM techniques permit evaluation of non-parametric criteria based upon bootstrapping and blindfolding to assess models (Hair, Hult, Ringle and Sarstedt, 2013).

The appropriateness of PLS-SEM for this research was assessed using rules of thumb suggested by Hair et al (2011). Specifically, the research goals of this study aim to extend current theory by predicting a key target construct (OSN CPM) and as such, PLS-SEM should be selected. PLS-SEM is also appropriate where complex structural models with many constructs and many indicators are specified. Hair et al (2011) do not elaborate on what constitutes 'many' constructs and indicators, but we conclude that the conceptual model in this study constitutes a complex structure as it has 82 indicator variables and 7 latent constructs, two of which are hierarchical. Furthermore, analysis of the data presented in the next chapter will reveal that the data are non-normal. Covariance Based SEM requires data be normally distributed, but PLS-SEM makes no such demands. Thus, PLS-SEM was determined to be a preferred analytic technique for this study.

5.5 Concluding Remarks

This chapter has outlined the positivist research philosophy that guided the Project and discussed the operationalization of key constructs under investigation – Objective Knowledge, Subjective Knowledge, Concern for Information Privacy, Trust in All Members, Trust in Close Connections, Trust in OSN Provider and

Online Social Network Communication Privacy Management. The chapter also offered a description of and justification for the nonprobability sampling technique employed and concluded with a description of the data analysis procedure that was undertaken. The next chapter, then, will present the results of the data analysis beginning with descriptive results derived through analysis using SPSS v. 19 and then measurement model and structural model results derived through analysis using SmartPLS v. 2.0.

6 Results

Study data collected via nonprobability sampling techniques discussed in Chapter 5 was analysed in two ways. Descriptive statistics were calculated using SPSS v. 19 and assessed. These results have been presented in Section 6.1. The conceptual model was tested using SmartPLS 2.0. Results of PLS-SEM testing have been presented in Section 6.2.

6.1 Descriptive Results

Descriptive results have been presented according to latent construct. Objective Knowledge (OK) was measured via a nominal scale with responses of true, false, or don't know. Thus, Objective Knowledge descriptive statistics are presented by frequency of response per variable. All other reflective latent constructs used 7 point Likert-scales and so other descriptive statistics including mean, standard error and standard deviation have been presented for those variables.

Normality was tested using the Shapiro-Wilk's W test where significance statistics greater than 0.05 are indicative of normal distributions (Field, 2005). All variables in this analysis were non-normal. Although this finding may be due in part to the relatively large sample size (N=835), examination of variable histograms suggested that many variables were indeed non-normal. As such, the median was presented for each variable in addition to the mean.

6.1.1 Objective Knowledge

Examination of responses to Objective Knowledge (OK) items illustrated that privacy knowledge among respondents was basic. Collectively, respondents were divided on their Objective Knowledge test performance. Approximately fifty per cent of the sample answered at least half of the questions correctly whereas the remaining 50 per cent of the sample answered less than half of the questions correctly. This means that if we were to apply North American academic passing grade standards to these results, we would conclude that half of respondents failed the test. Providing an option to admit not knowing an answer should have minimised the likelihood of respondent guessing. As such, correct answers should have more closely reflected genuine accuracy of Objective Knowledge while incorrect answers and admissions of ignorance combined should have reflected authentic lack of knowledge.

A small minority of the sample (7%) scored a 0 on the Objective Knowledge (OK) quiz indicating complete ignorance about privacy. This result could have been achieved either by respondents selecting ‘Don’t Know’ for every answer or by answering each of the 10 questions incorrectly (i.e. selecting ‘True’ when the correct answer was ‘False’). Visual inspection of responses to the OK scale revealed that 45 respondents (5%) selected ‘Don’t Know’ for all ten questions. It is possible that some or all of these individuals selected the option without reflecting upon the question, but that cannot be determined from the data.

From the frequency distribution of answers we are able to identify privacy topics about which respondents admit being ignorant. A majority of respondents

(57%) admitted not knowing about video surveillance protections under PIPEDA (Q6). Other questions for which the largest proportions of the sample not knowing answers were observed included: Q4 (48%) pertaining to the scope of PIPEDA, Q3 (38%) pertaining to photocopying personally identifiable documentation, and Q8 (35%) which asked about the proper privacy complaint channel. Further, sizeable proportions of respondents demonstrated clear inaccuracy in responses to Q10 (56% incorrect), Q1 (47% incorrect), Q2 (41% incorrect), and Q3 (28% incorrect).

Examination of the frequency distribution of answers (Table 6.1.) indicated there were some aspects of privacy about which respondents were knowledgeable, but others about which they were generally less knowledgeable. Most respondents knew what constituted a privacy breach (75%), were aware that one's Social Insurance Number cannot be collected by all organizations with which one interacts (71%) and recognised that law enforcement officials have the ability to access one's personal information held with organisations without consent (64%). Slightly more than half of respondents were aware that they may complain to the Office of the Privacy Commissioner when denied access to their personal information (57%). However, only a minority of respondents answered six questions correctly. Generally speaking, respondents were unfamiliar with the general areas of personal information coverage offered by PIPEDA (Q4), the protections associated with video surveillance (Q6) and photocopying personally identifiable documentation (Q3), and the particulars of informed consent (Q1, Q2 and Q10).

Table 6.1 Frequency Distribution of Objective Knowledge Variables

Variable (Correct Answer)	n	True	False	Don't Know
1. To get your permission to capture your personal information, an organization only needs to tell you the purposes for which the information will be used. **(False)**	835	397 47.5%	216 25.9%	222 26.6%
2. Organizations can always refuse to supply a product or service if you won't give permission to the collection, use or disclosure of your personal information. **(False)**	835	341 40.8%	285 34.1%	209 25.0%
3. If an organization is required by law to record an identity document number, like a driver's license number, the document should always be photocopied by the organization. **(False)**	835	229 27.4%	293 35.1%	313 37.5%
4. Canada's Personal Information Protection and Electronics Documents Act (PIPEDA) covers the collection, use or disclosure of personal information by organizations in the course of commercial activity. **(True)**	835	365 43.7%	71 8.5%	399 47.8%
5. All Canadian organizations can collect your Social Insurance Number so they can identify you. **(False)**	835	101 12.1%	597 71.5%	137 16.4%
6. An organization, which is subject to PIPEDA, uses overt video surveillance for justified security and crime prevention reasons but does not record any images. Since no images are recorded, compliance with PIPEDA is not an issue. **(False)**	835	90 10.8%	267 32.0%	478 57.2%
7. A privacy breach has occurred when there is unauthorized access to, or collection, use, or disclosure of personal information. **(True)**	835	624 74.7%	50 6.0%	161 19.3%
8. An individual can make a complaint to the Office of the Privacy Commissioner of Canada against an organization if an organization denies them access to their personal information. **(True)**	835	478 57.2%	64 7.7%	293 35.1%
9. Under certain circumstances, an organization can disclose their customer's personal information to law enforcement officials without their customer's consent. **(True)**	835	531 63.6%	103 12.3%	201 24.1%
10. When recording customer telephone calls, organizations must inform the individual that the call may be recorded but not the purposes for which the information will be used. **(False)**	835	472 56.5%	218 26.1%	145 17.4%

6.1.2 Subjective Knowledge

Subjective Knowledge (SK) responses ranged from a minimum of 1 to a maximum of 7. A review of Subjective Knowledge descriptive statistics (Table 6.2) revealed that respondents perceived their knowledge about personal information privacy to be approximately neutral on each of the SK observed measures (M = 4.16, 4.03 and 3.79 for SK 1, 2 and 3, respectively). Comparison of the means for each of the SK items in Table 6.2 suggests that respondents generally were more confident in their privacy knowledge compared to personal reference groups, were reasonably confident they know about how organisations collect and manage their data, but had less confidence in their knowledge about personal information privacy in OSNs. Examination of frequency distributions revealed that the majority of respondents had either low Subjective Knowledge (41% had SK scores between 1 and 3) or neutral Subjective Knowledge (33% had SK scores = 4). Only 26% rated their knowledge at the higher end of the scale (scores of 5, 6 or 7). These results revealed that, for the sample, Subjective Knowledge was not high.

Table 6.2 Descriptive Statistics for Subjective Knowledge

Variable	N	Min	Max	Mean	Median	SE	SD
Compared to most people you know, how would you rate your knowledge about how organizations collect and manage your personal information?	835	1	7	4.16	4.00	.047	1.351
In general, I am quite knowledgeable about how organizations collect and manage my personal information.	835	1	7	4.03	4.00	.051	1.471
I am quite knowledgeable about how the information I provide in my online social network is collected and managed by companies.	835	1	7	3.79	4.00	.053	1.546

6.1.3 Concern for Information Privacy

Concern for Information Privacy (CFIP) responses ranged from a minimum of 1 to a maximum of 7 on each item. Respondents' concern about each aspect of information privacy would be classified as high as indicated by means of each items exceeding the neutral point of 4. In particular, the median response for all Improper Access and Unauthorised Secondary Use variables was the maximum score of 7.

Skewness measures of + or – 1 indicate the data is skewed (Hair, Black, Babin and Anderson, 2010). Similarly, kurtosis statistics of + or -1 signify kurtotic data. Review of variable skewness and kurtosis results (Table 6.4) show that all CFIP variables except E1 are skewed to the far right of neutral, meaning that privacy concerns are very high among the sample. Kurtosis statistics reveal that concern about errors, is relatively flatly distributed at the higher end of a normal distribution curve and concern about collection is highly kurtotic for C2 and kurtotic for C3. All IA and USU measures were highly kurtotic. These measures indicate that most respondents are highly concerned about all aspects of improper access and unauthorised secondary use of their personal information.

While one of the advantages of PLS is its ability to handle non-normal data, data as skewed and kurtotic as evidenced here might be problematic (Hair, Hult, Ringle and Sarstedt, 2013).

Table 6.3 Descriptive Statistics for Concern for Information Privacy

Variable		N	Min	Max	Mean	Median	SE	SD
Collection								
C1	It usually bothers me when companies ask me for personal information.	835	1	7	5.58	6	.054	1.551
C2	When companies ask me for personal information, I sometimes think twice before providing it.	835	1	7	6.30	7	.041	1.194
C3	It bothers me to give personal information to so many companies.	835	1	7	5.98	7	.047	1.366
C4	I'm concerned that companies are collecting too much personal information about me.	835	1	7	5.74	6	.052	1.496
Improper Access								
IA1	Companies should devote more time and effort to preventing unauthorized access to personal information.	835	1	7	6.23	7	.043	1.244
IA2	Computer databases that contain personal information should be protected from unauthorized access – no matter how much it costs.	835	1	7	6.22	7	.045	1.301
IA3	Companies should take more steps to make sure that unauthorized people cannot access personal information in their computers.	835	1	7	6.33	7	.041	1.174
Unauthorised Secondary Use								
USU1	Companies should not use personal information for any purpose unless it has been authorized by the individuals who provided the information.	835	1	7	6.37	7	.043	1.229
USU2	When people give personal information to a company for some reason, the company should never use the information for any other reason.	835	1	7	6.26	7	.046	1.315
USU3	Companies should never sell the personal information in their computer databases to other companies.	835	1	7	6.35	7	.044	1.258
USU4	Companies should never share personal information with other companies unless it has been authorized by the individuals who provided the information.	835	1	7	6.47	7	.039	1.135
Errors								
E1	All the personal information in computer databases should be double-checked for accuracy – no matter how much this costs.	835	1	7	4.88	5	.060	1.725

E2	Companies should take more steps to make sure that the personal information in their files is accurate.	835	1	7	5.60	6	.053	1.535
E3	Companies should have better procedures to correct errors in personal information.	835	1	7	5.59	6	.052	1.510
E4	Companies should devote more time and effort to verifying the accuracy of the personal information in their databases.	835	1	7	5.54	6	.053	1.541

Table 6.4 CFIP Skewness and Kurtosis

Variable	Skewness		Kurtosis	
	Statistic	Std. Error	Statistic	Std. Error
Collection				
C1	-1.060	.085	.473	.169
C2	-2.087	.085	4.490	.169
C3	-1.368	.085	1.352	.169
C4	-1.154	.085	.711	.169
Improper Access				
IA1	-1.828	.085	3.232	.169
IA2	-1.850	.085	2.963	.169
IA3	-2.013	.085	3.974	.169
Unauthorised Secondary Use				
USU1	-2.199	.085	4.489	.169
USU2	-1.961	.085	3.379	.169
USU3	-2.136	.085	4.179	.169
USU4	-2.454	.085	5.905	.169
Errors				
E1	-.392	.085	-.705	.169
E2	-1.021	.085	.386	.169
E3	-.992	.085	.373	.169
E4	-.983	.085	.378	.169

6.1.4 Trust

Trust item responses ranged from a minimum of 1 to a maximum of 7 on each item and are shown in Tables 6.5 (TP), 6.6 (TAM) and 6.7 (TCC). It appeared as though respondents had a reasonable amount of trust in their OSN service providers as indicated by TP means ranging from 3.76 to 4.12. Trust in all members of an OSN was generally higher than that with the OSN provider (means ranging from 4.43 to 4.84). Trust in respondents' close connections was highest with means ranging from 5.57 to 5.74. Trust in close connections variables were skewed to the right of normal as indicated by skewness statistics of -1.205, -1.049, -1.017, -.959, -.919, -1.034 for TCC1 through TCC 6, respectively. TCC1, TCC2 and TCC3 were determined to be kurtotic as well, with kurtosis statistics of 1.405, .999, and 1.073, respectively.

Table 6.5 Descriptive Statistics for Trust in Provider Variables

Variable	N	Min	Max	Mean	Median	SE	SD
My online social network company…							
...is open and receptive to the needs of its members.	835	1	7	4.12	4.00	.051	1.480
...makes good-faith efforts to address most members' concerns.	835	1	7	4.09	4.00	.051	1.470
...is also interested in the well-being of its members, not just its own.	835	1	7	3.78	4.00	.053	1.544
...is honest in its dealings with me.	835	1	7	3.93	4.00	.052	1.500
...keeps its commitments to its members.	835	1	7	4.11	4.00	.051	1.478
...is trustworthy.	835	1	7	3.76	4.00	.057	1.651

Table 6.6 Descriptive Statistics for Trust in All Members Variables

Variable	N	Min	Max	Mean	Median	SE	SD
Generally speaking, all my friends and connections...							
...will do their best to help me.	835	1	7	4.55	5.00	.051	1.488
...do care about the well-being of others.	835	1	7	4.84	5.00	.047	1.356
...are open and receptive to the needs of each other.	835	1	7	4.72	5.00	.046	1.327
...are honest in dealing with each other.	835	1	7	4.52	4.00	.049	1.409
...keep their promises.	835	1	7	4.43	4.00	.047	1.368
...are trustworthy.	835	1	7	4.56	5.00	.048	1.393

Table 6.7 Descriptive Statistics for Trust in Close Connections Variables

Variable	N	Min	Max	Mean	Median	SE	SD
The friends and connections I share the most information with...							
...will do their best to help me.	835	1	7	5.74	6.00	.046	1.316
...do care about the well-being of others.	835	1	7	5.72	6.00	.043	1.253
...are open and receptive to the needs of each other.	835	1	7	5.67	6.00	.043	1.238
...are honest in dealing with each other.	835	1	7	5.60	6.00	.045	1.294
...keep their promises.	835	1	7	5.57	6.00	.045	1.299
...are trustworthy.	835	1	7	5.66	6.00	.045	1.306

6.1.5 OSN Communication Privacy Management

OSN Communication Privacy Management (OSN CPM) was measured on three separate dimensions of Boundary Ownership, Boundary Linkages and Boundary Permeability with 36 variables. All OSN CPM item responses ranged from a minimum of 1 to a maximum of 7 and are shown in Tables 6.8 (BO), 6.9 (BL) and 6.10 (BP).

The Boundary Ownership measure was intended to reflect how individuals' control their personal information boundaries with respect to information ownership. This scale was reverse coded. If an individual holds personal information ownership boundaries tightly, then scores on the reversed scale should be low (less than 4). Review of descriptive statistics presented in Table 6.8 suggests there are some areas of personal information where boundaries are held more tightly than others. For instance, as indicated by mean values, boundary ownership appeared to not be held tightly for personal identifiers like birthdate (BO10, M=4.65), real name (BO12, M=6.33), photo sharing (BO8, M=5.03 and BO7, M=4.48). Personal contact information (BO9) was viewed more neutrally by the study sample as a whole

Table 6.8 Descriptive Statistics for Boundary Ownership (Reverse Coded) Variables

Variable		N	Min	Max	Mean	Median	SE	SD
BO1	I have limited the personal information posted on my profile.*	835	1	7	2.25	2.00	.053	1.531
BO2	I use shorthand (e.g., aliases or limited details) when discussing sensitive information so others have limited access to my personal information.*	835	1	7	4.27	4.00	.077	2.226
BO3	If I think that information I posted really looks too private, I might delete it.*	835	1	7	2.30	1.00	.065	1.891
BO4	I am slow to talk about recent events because people might talk.*	835	1	7	4.15	4.00	0.071	2.062
BO5	I don't post about certain topics because I worry who can see it.*	835	1	7	2.57	2.00	0.064	1.859
BO6	Seeing intimate details about someone else makes me feel I should keep their information private.*	835	1	7	3.61	4.00	0.069	1.999
BO7	I never tag friends in photos.*	835	1	7	4.48	5.00	.072	2.075
BO8	When I am tagged in a photo I remove it immediately.*	835	1	7	5.03	5.00	.062	1.723
BO9	I do not share any of my contact information in my profile.*	835	1	7	3.58	4.00	.069	1.999
BO10	My birth date is not visible on my profile.*	835	1	7	4.65	6.00	.086	2.496
BO11	I like to put my connections in groups so that different people can see different things.*	835	1	7	5.71	6.00	.060	1.732
BO12	I have changed my name on my profile to prevent certain people from finding me.*	835	1	7	6.33	7.00	.054	1.546

(M=3.58, SD=1.999). Responses also indicate little preference for grouping OSN connections to control who has access to what personal information (BO11, M=5.71). On the other hand, boundary ownership rules appear to be exercised via self-censorship with respect to the amount of information provided on one’s profile (BO1), deleting information upon reflection (BO3), and exercising restraint in the information posted (BO5). Respondents were generally neutral about using shorthand (BO2), and contemplating sharing information that would likely be shared (BO4).

The Boundary Linkages measure was intended to reflect how open OSN users were with connecting (or linking) to others in the network. An individual who exercises strict control over their personal information will be less likely to link via the items measured in the scale. Thus, disagreement with the linkage items suggests less connection or tighter control of boundary linkages and will be represented in the scale by BL scores less than 4. Review of descriptive statistics presented in Table 6.9 suggests that, overall, boundary linkages were tightly held by respondents as evidenced by mean scores ranging from 1.98 (BL5) to 3.94 (BL8).

Table 6.9 Descriptive Statistics for Boundary Linkages Variables

Variable		N	Min	Max	Mean	Median	SE	SD
BL1	I have created a detailed profile so that others can link to me with similar interests.	835	1	7	2.45	2	.056	1.610
BL2	I try to let people know my best activities and interests so I can find friends.	835	1	7	2.21	2	.055	1.594
BL3	I allow people with a profile or picture I like to access my profile.	835	1	7	2.27	1	.063	1.806
BL4	I comment on or like things on friends' pages to have others check out my profile.	835	1	7	2.39	2	.063	1.832
BL5	I have my privacy settings set to 'Everyone'.	835	1	7	1.98	1	.064	1.849
BL6	I like to link to interesting websites to increase traffic on my profile.	835	1	7	2.24	1	.060	1.728
BL7	I use social networking links (like the Facebook 'like' button) on other websites.	835	1	7	3.11	3	.070	2.015
BL8	I support companies and people by 'liking' pages or making recommendations.	835	1	7	3.94	4	.066	1.919
BL9	I accept most friend or connection requests I receive.	835	1	7	3.62	4	.060	1.720
BL10	I like to add 'applications' to improve my experience.	835	1	7	2.22	2	.056	1.616
BL11	I feel uncomfortable saying no to 'friend' requests.	835	1	7	3.11	2	.076	2.192
BL12	I have a limited profile that only allows very close connections to see my detailed information.*	835	1	7	2.99	2	.073	2.116

The Boundary Permeability measure was intended to reflect the breadth and depth of information OSN users shared with others in their network. An individual who exercises more communication privacy management would be less likely to share large amounts of personal information of the types identified by scale items. Thus, disagreement with the permeability items suggests less information sharing or less permeable boundaries and will be represented in the scale by BP scores less than 4. Review of descriptive statistics presented in Table 6.10 suggests that, overall, boundaries of the study sample were not very permeable as evidenced by mean scores ranging from 1.60 (BP4) to 3.94 (BP8). Mean scores of BP items further indicated that respondents were generally more likely to share positive news (BP8, M=3.94), frequently update OSN statuses (BP6, M=3.28), and profiles (BP6, M=3.13) and share feelings (BP9, M=3.00). But, the information shared is less likely to be negative (BP1, M=2.71; BP3, M=1.70), work related (BP3, M=1.70), about close friends (BP11, M=1.53) or intimate (BP4, M=1.60). Even when upset by a company, respondents were not very likely to post about the incident in OSNs (BP12, M=2.52).

Table 6.10 Descriptive Statistics for Boundary Permeability Variables

Variable		N	Min	Max	Mean	Median	SE	SD
BP1	When I face challenges in my personal life, I feel comfortable talking about them.	835	1	7	2.71	2	.063	1.820
BP2	I like my status updates or posts to be long and detailed.	835	1	7	2.09	2	.050	1.450
BP3	I like to discuss work concerns publicly.	835	1	7	1.70	1	.046	1.343
BP4	I often tell intimate, personal things without hesitation.	835	1	7	1.60	1	.045	1.313
BP5	I share information with people whom I don't know in my day-to-day life.	835	1	7	2.30	1	.061	1.765
BP6	I update my profile frequently.	835	1	7	3.13	3	.062	1.803
BP7	I update my status frequently.	835	1	7	3.28	3	.067	1.922
BP8	When something positive happens to me, I post about it.	835	1	7	3.94	4	.063	1.818
BP9	My status updates generally indicate how I am feeling.	835	1	7	3.00	3	.061	1.748
BP10	I like to provide detailed comments on friends' pages.	835	1	7	2.78	3	.054	1.572
BP11	When a friend in my network upsets me, I post about it.	835	1	7	1.53	1	.039	1.135
BP12	When a business or company upsets me, I post about it.	835	1	7	2.52	2	.063	1.825

6.2 Partial Least Squares Results

Prepared data were imported into SmartPLS, the conceptual model (Figure 4.1) was specified and the PLS algorithm was run with path weighting scheme settings, Data Metric of Mean 0, Var 1, 300 maximum iterations, abort criterion of 1.0 E-5 and initial weights of 1.0. There were no missing values in the data. The bootstrapping algorithm was also run with cases equal to 835 (equal to the sample size), 5000 samples and no sign changes specified. Results of the hypothesised model, presented in Section 6.2.1, were analysed. Based upon analysis of the hypothesised model, small changes were made to the model and PLS and bootstrapping algorithms re-run with the same settings and results analysed. This process continued until a final model was achieved. Results of the final model are presented in Section 6.2.2.

6.2.1 Hypothesised model

The hypothesised model converged after 13 iterations with the PLS algorithm. Results of the PLS algorithm are shown in Figure 6.1. Values shown in the circular latent constructs represent the coefficient of determination (R^2), values on the paths represent the standardised path coefficients and have been denoted with indications of significance. Table 6.11 provides a table of path coefficients and significance values as well.

From a cursory review of the PLS algorithm results, all hypothesised paths except that from CFIP to TP were significant. The path from CFIP → TAM was significant at a level of $p < .05$, the path from OK → CFIP was significant at a level of $p < .01$ and all other significant paths were highly significant ($p < .001$). Despite their significance, paths were weak predictors of endogenous latent constructs. To be accepted, the coefficient of determination (R^2) of endogenous constructs must meet or exceed a threshold of .10 (Falk and Miller 1992). OK and SK explained

Figure 6.1 Hypothesised Model Evaluation

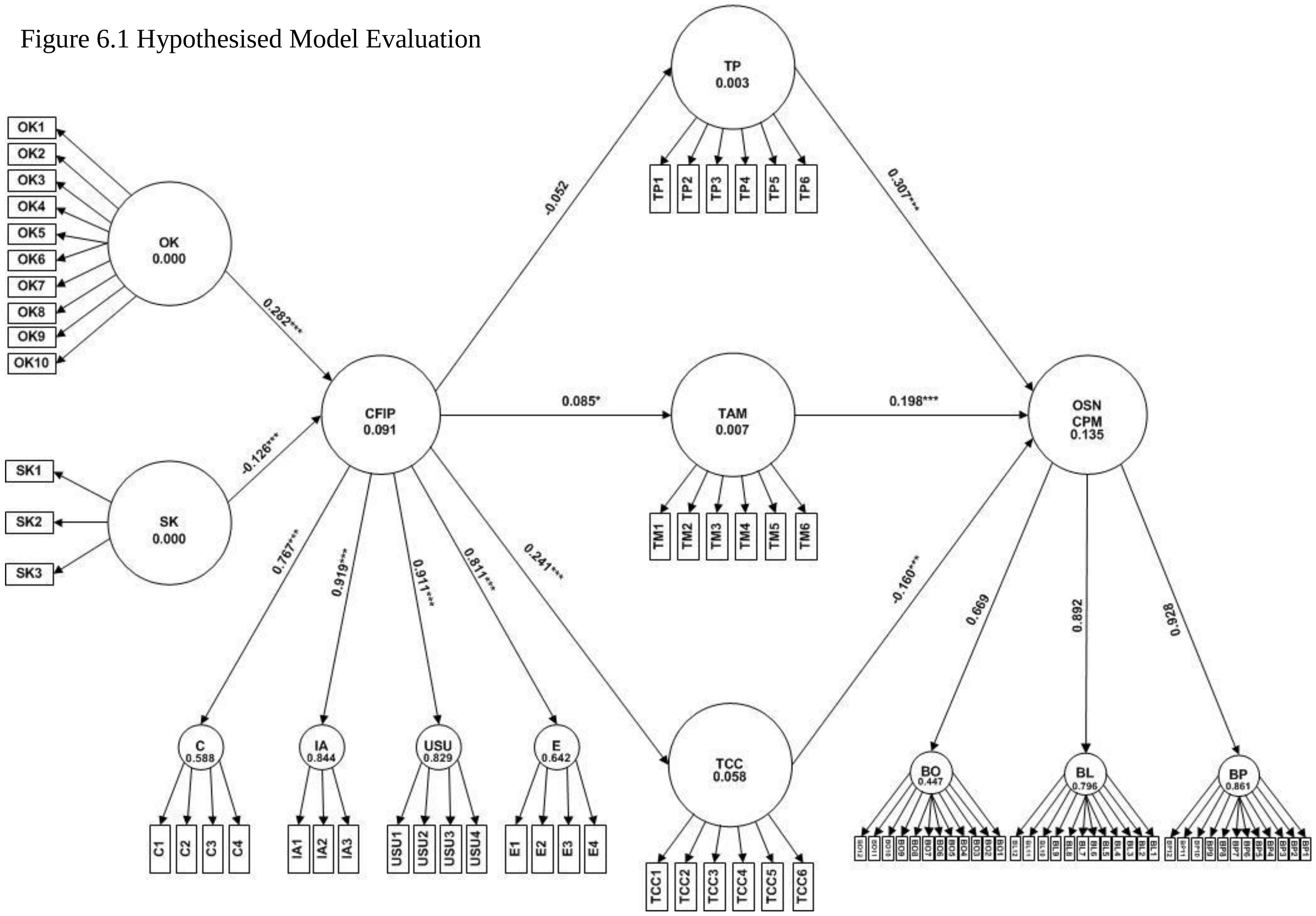


Table 6.11 Path Coefficients and Significance of Hypothesised Model

Path	Path Coefficient	Empirical t value	Critical t value	p value
CFIP -> C	0.791	36.149	***	0.000
CFIP -> E	0.793	44.977	***	0.000
CFIP -> IA	0.916	126.506	***	0.000
CFIP -> TAM	0.085	2.192	*	0.029
CFIP -> TCC	0.241	5.734	***	0.000
CFIP -> TP	-0.052	1.280	NS	0.201
CFIP -> USU	0.908	101.835	***	0.000
OSN CPM -> BL	0.892	84.502	***	0.000
OSN CPM -> BP	0.928	109.996	***	0.000
OSN CPM -> BO	0.669	27.860	***	0.000
OK -> CFIP	0.282	3.239	**	0.001
SK -> CFIP	-0.125	3.679	***	0.000
TAM -> OSN CPM	0.198	3.988	***	0.000
TCC -> OSN CPM	-0.160	3.802	***	0.000
TP -> OSN CPM	0.307	7.927	***	0.000

NS = not significant

only 9% of the variance of CFIP (R^2=.091). CFIP explained virtually none of the variance in trust in the provider (TP R^2=.003) or trust in all members (TAM R^2=.007) and only 6% of the variance in trust in close connections (TCC R^2=.058). The three trust constructs (TP, TAM and TCC) combined to explain only 13% of the variance in OSN CPM (R^2=.135). Therefore, the results of the tests of the hypothesised model suggested some basic support for all hypothesised relationships, but not all anticipated relationships could be concluded given the predictive capability of the observed statistics.

Extensive interpretation of the model was not required until reliability and validity of constructs had been assessed, however. A summary of composite reliability and convergent validity measures of the hypothesised model has been presented in Table 6.12.

Internal consistency reliability, or the extent to which the measures consistently represent the same latent construct, was assessed with composite reliability measures generated by Smart PLS software. Composite reliability (CR) values vary between 0 and 1, with acceptable values for exploratory research considered to be between 0.60 and 0.70 (Hair et al 2013). CR values between 0.708 and 0.90 are considered high while values in excess of .95 may present validity problems.

Examination of CR values of the hypothesised model indicated that CFIP (CR = 0.9446) and each of its dimensions – C (CR = 0.8955), IA (CR = 0.9293), USU (CR = 0.9218) and E (CR = 0.9442) had acceptable composite reliabilities. Similarly, SK, TP, TAM, and TCC all had acceptable CR values, each in excess of 0.9090. The composite reliability of OSN CPM was also acceptable (CR = 0.8584), but the CR of the BO dimension was well below even the lowest recommended level of 0.60 (CR = 0.1449). The CR of OK was slightly below an accepted level for exploratory research (CR = 0.5439).

Convergent validity, or the extent to which a measure correlates positively with other measures of the same construct, was assessed with outer loading statistics and AVE measures (Hair et al, 2013). Outer loadings are typically accepted at a level of 0.70, but social science research, particularly exploratory investigations, will often accept outer loadings at a level of 0.4. Two other criteria have also been recommended to conclude convergent validity: 1) AVE must be greater than 0.50

and 2) composite reliability must be greater than AVE. AVE values of at least 0.50 are considered acceptable because at 0.50, the construct is thought to explain half of the variance of its indicators. And, when the internal consistency reliability exceeds the variance extracted by the measures, the researcher can be better assured that the variance observed is correctly attributed to the intended measure.

All outer loadings of trust constructs (TP, TAM and TCC), the CFIP construct and its first order constructs (C, IA, USU, and E) and SK were above the minimum cut-off of 0.40 for exploratory research and AVE values exceeded the 0.50 threshold. Within the first order constructs of OSN CPM, all BP indicators met the minimum loading cut-off criterion, but five BO variables (BO1, BO5, BO8, BO9 and BO11) and two BL variables (BL11 and BL12) fell below the threshold. AVE values for BO, BL, BP and the second order construct of OSN CPM (AVE = 0.1315, 0.3215, 0.4176, and 0.2226, respectively) suggested the constructs as hypothesised were problematic. Similarly, the new construct of OK showed five manifest variables with poor outer loadings (OK1, OK3, OK4, OK6 and OK10). An AVE on the OK construct of 0.1785 coupled with the poor loading variables suggested that the ten manifest variables were not all converging on OK.

Table 6.12 Results Summary for Hypothesised Model

Latent Variable	Indicators	Loadings	Indicator Reliability (Item communality)	Higher Order Item Loading	Composite Reliability	AVE	Discriminant Validity
OK	OK1	-0.2650	0.0702		0.5439	0.1785	
	OK2	0.6640	0.4409				
	OK3	0.1374	0.0189				
	OK4	0.2278	0.0519				
	OK5	0.5967	0.3561				
	OK6	0.1845	0.0340				
	OK7	0.8460	0.7157				
	OK8	0.5845	0.3416				
	OK9	0.5111	0.2612				
	OK10	0.2500	0.0625				

SK	SK1	0.8941	0.7994		0.9090	0.7692	
	SK2	0.8929	0.7973				
	SK3	0.8431	0.7108				
				CFIP	0.9446	0.5528	
C	C1	0.7650	0.5852	0.5880	0.8955	0.6825	Yes
	C2	0.8151	0.6644	0.6721			
	C3	0.8925	0.7966	0.6943			
	C4	0.8270	0.6839	0.8216			
IA	IA1	0.8962	0.8032	0.8364	0.9293	0.8142	Yes
	IA2	0.9125	0.8327	0.8225			
	IA3	0.8983	0.8069	0.7550			
USU	USU1	0.8444	0.7130	0.8116	0.9218	0.7466	
	USU2	0.8648	0.7479	0.7765			
	USU3	0.8563	0.7332	0.7961			
	USU4	0.8910	0.7939	0.6680			
E	E1	0.8520	0.7259	0.7362	0.9442	0.8095	Yes
	E2	0.9234	0.8527	0.7597			
	E3	0.9277	0.8606	0.7413			
	E4	0.9360	0.8761	0.5880			
TP	TP1	0.8490	0.7208		0.9502	0.7608	
	TP2	0.8758	0.7670				
	TP3	0.8784	0.7716				
	TP4	0.8885	0.7894				
	TP5	0.9270	0.8593				
	TP6	0.8456	0.7150				
TAM	TAM1	0.8671	0.7519		0.9596	0.7984	
	TAM2	0.8849	0.7830				
	TAM3	0.9186	0.8438				
	TAM4	0.8991	0.8084				
	TAM5	0.9118	0.8314				
	TAM6	0.8785	0.7718				
TCC	TCC1	0.9134	0.8343		0.975	0.8666	
	TCC2	0.9438	0.8908				
	TCC3	0.9529	0.9080				
	TCC4	0.9268	0.8590				
	TCC5	0.9291	0.8632				
	TCC6	0.9190	0.8446				
				OSN CPM	0.8584	0.2226	
BO	BO1	0.4788	0.2292	0.2859	0.1449	0.1315	No
	BO2	-0.2950	0.0870	-0.1913			
	BO3	0.3294	0.1085	0.1394			
	BO4	0.3470	0.1204	0.1734			
	BO5	0.4235	0.1794	0.2259			
	BO6	0.1662	0.0276	-0.1100			
	BO7	0.2183	0.0477	0.8250			
	BO8	0.8490	0.7208	0.3300			
	BO9	0.4385	0.1923	0.2225			
	BO10	0.0977	0.0095	0.2140			
	BO11	-0.7420	0.5506	-0.5521			
	BO12	-0.3414	0.1166	-0.2710			
BL	BL1	0.6920	0.4789	0.6310	0.8384	0.3215	No
	BL2	0.7275	0.5293	0.6643			

	BL3	0.6190	0.3832	0.5146			
	BL4	0.6770	0.4583	0.5761			
	BL5	0.5120	0.2621	0.4118			
	BL6	0.7216	0.5207	0.6551			
	BL7	0.5625	0.3164	0.5342			
	BL8	0.5118	0.2619	0.4854			
	BL9	0.4181	0.1748	0.3354			
	BL10	0.6275	0.3938	0.5794			
	BL11	0.2316	0.0536	0.1939			
	BL12	0.2143	0.0459	0.1362			
BP	BP1	0.6200	0.3844	0.5523	0.8952	0.4176	No
	BP2	0.7530	0.5670	0.6510			
	BP3	0.6296	0.3964	0.6390			
	BP4	0.6784	0.4602	0.6367			
	BP5	0.5129	0.2631	0.5513			
	BP6	0.6718	0.4513	0.6189			
	BP7	0.7248	0.5253	0.6276			
	BP8	0.6555	0.4297	0.5746			
	BP9	0.6720	0.4516	0.5729			
	BP10	0.6288	0.3954	0.6840			
	BP11	0.6191	0.3833	0.6155			
	BP12	0.6130	0.3758	0.5272			

Discriminant validity, or the extent to which constructs are distinct from one another, was determined by comparing √AVE with latent variable correlations according to Fornell-Larcker criteria (Hair et al 2013). In the Fornell-Larcker test, discriminant validity may be concluded when the √AVE of a construct is: 1) greater than 0.707 and 2) greater than the construct's correlation coefficient with any other construct. The Fornell-Larcker test has been presented in Table 6.13.

The Fornell-Larcker criteria suggested that the BL and BP constructs were not sufficiently discriminated as specified in the hypothesised model where each measure consisted of twelve manifest items. Similarly, BO was not discriminant from the other OSN CPM constructs. Each of the three trust constructs (TP, TAM and TCC), the privacy literacy constructs (OK and SK) and the higher order CFIP construct were discriminant from all other constructs in the model. (It should be noted that the first order constructs of CFIP were not discriminant from the higher order CFIP construct, but this was not a requirement.)

Table 6.13 Fornell-Larcker Criteria for Hypothesised Model

(Shaded value on the diagonal represents √AVE)

	BL	BP	C	CFIP	E	IA	BO	OSN CPM	OK	SK	TAM	TCC	TP	USU
BL	.567													
BP	0.684	.646												
C	-0.221	-0.243	.826											
CFIP	-0.151	-0.168	0.791	.744										
E	-0.230	-0.785	0.489	0.793	.900									
IA	-0.124	-0.135	0.673	0.916	0.617	.902								
BO	0.531	0.529	-0.287	-0.274	-0.151	-0.238	.363							
OSNCPM	0.892	0.928	-0.253	-0.240	-0.749	-0.164	0.669	.472						
OK	-0.118	-0.180	0.196	0.274	0.134	0.299	-0.168	-0.136	.422					
SK	0.184	0.236	-0.112	-0.164	-0.694	-0.567	0.172	0.234	0.066	.877				
TAM	0.177	0.199	0.544	0.852	0.871	0.827	0.264	0.193	0.117	0.093	.894			
TCC	-0.130	0.690	0.179	0.241	0.138	0.268	-0.187	0.146	0.173	0.793	0.554	.931		
TP	0.360	0.266	-0.121	-0.518	0.130	-0.346	0.144	0.326	-0.155	0.714	0.264	0.211	.827	
USU	-0.185	-0.183	0.673	0.976	0.562	0.831	-0.294	-0.224	0.296	-0.137	0.576	0.231	-0.6	.864

Assessment of the results of the measurement model, as above, suggested a number of modifications be made to the exploratory constructs under investigation in the measurement model in order to achieve composite reliability and convergent and discriminant validity. Thus, minor modifications were made to the model via trimming manifest variables, re-running the PLS algorithm and reassessing the measurement model. The PLS Algorithm was also run in conjunction with these tests to assess the significance of path relationships within the structural model and insignificant paths were dropped in a sequential manner. As a result of poor levels of

R^2 for the hypothesised endogenous location of trust and CFIP constructs, the exploratory nature of this investigation and support within the literature, TP, TCC and CFIP were made exogenous constructs to predict OSN CPM. The test-re-test process just described also did not support treatment of the OSN CPM construct as a second order construct nor was the inclusion of BO as a distinct construct supported.

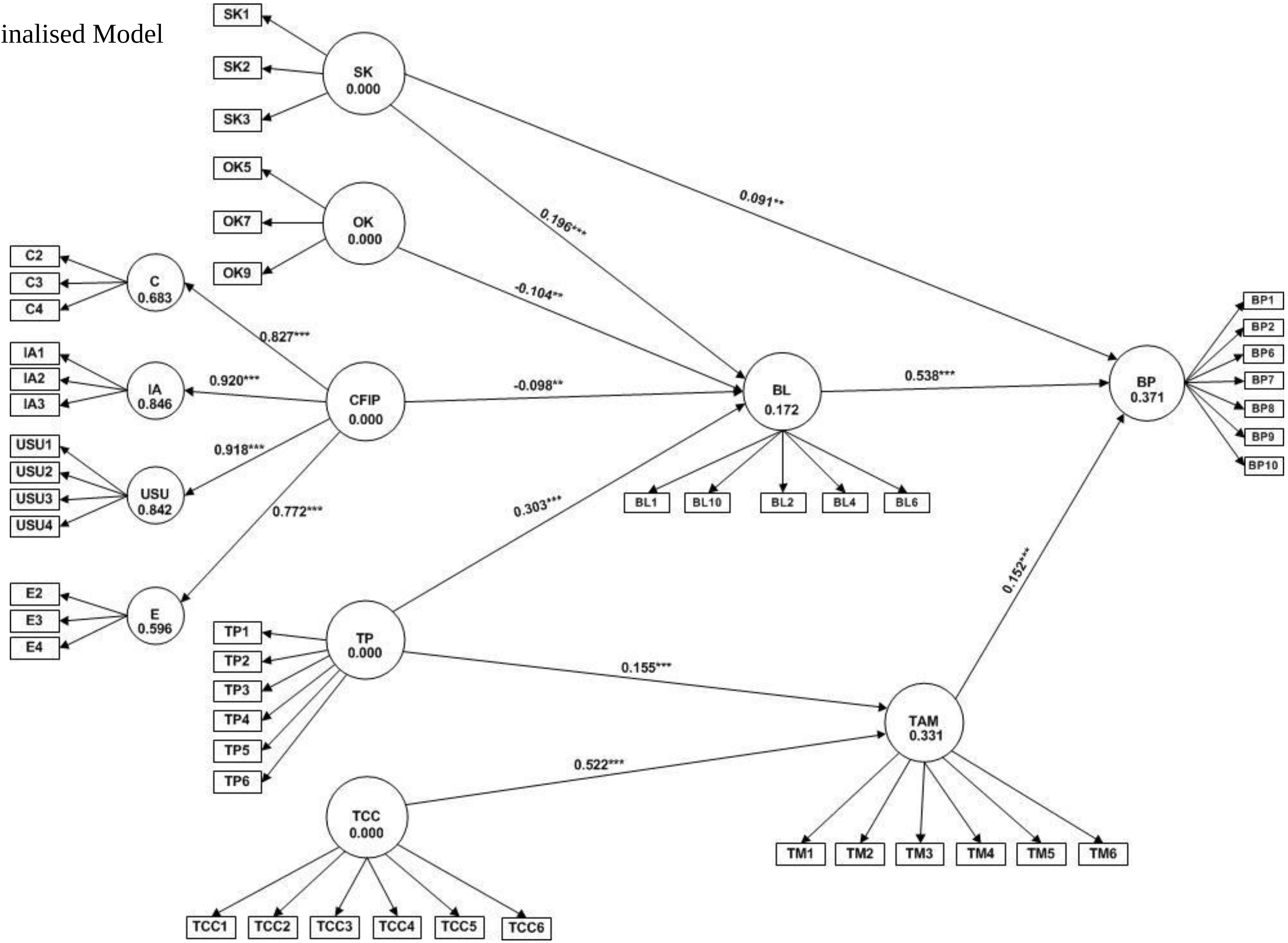
6.2.2 Final Model

The finalised model, presented in Figure 6.2, converged after 5 iterations with the PLS algorithm. Through the model development process the original hypothesised model evolved to that finally achieved (Figure 6.2) via modification of construct structure and respecification of paths. Alteration of the measurement model was guided by statistical results and those results have been presented in the following subsection entitled ‘Measurement Model’. The statistical results of the final model’s structure have been presented in the subsection ‘Structural Model’ wherein relationships between constructs have been assessed.

Measurement Model

To arrive at the final model a number of manifest variables were dropped in the process due to poor convergent validity, poor composite reliability, and/or poor discriminant validity. In each instance where manifest variable deletion was considered, the associated impact upon AVE was also assessed (Hair et al, 2013).

Figure 6.2. Finalised Model



Summarised results of the finalised measurement model have been presented in Table 6.14. These statistics indicated reliability of the constructs via composite reliability measures in excess of 0.70 in all instances, though the very high CR values associated with TP (CR = 0.9501), TAM (CR = 0.9597), TCC (CR = 0.9751) suggested caution was warranted due to potential problems with validity. Convergent validity of latent constructs was concluded via acceptable outer loadings on the constructs. No item recorded an outer loading lower than 0.5616 (OK9), but this value was well within acceptable limits for an exploratory construct (lower limit = 0.40) and further justified for retention given that removing the item offered no improvement to AVE and removal would result in an underidentified construct (Hair et al, 2010). The only outer loadings below 0.70 (but still within acceptable limits) were recorded for the other exploratory constructs of BL and BP. Specifically, these outer loadings were: 0.6877 for BL4, 0.6640 for BL10, 0.6793 for BP 10 and 0.6134 for BP1. Convergent validity was further supported by AVE values for all constructs exceeding the critical level of 0.50.

Discriminant validity of constructs within the final model was determined by comparing √AVE with latent variable correlations according to Fornell-Larcker criterion (Table 6.15) and was further confirmed via examination of item cross loadings (Table 6.16) following recommendations in Hair et al (2013). Accordingly, in cross-loading comparisons all items within a construct must load more strongly on its own construct than on any other construct within the measurement model. As with the hypothesised model, the first order constructs of CFIP were not discriminant from the higher order CFIP construct, but this was not a requirement. To demonstrate discriminant validity within a higher order construct, the first order

Table 6.14 Results Summary for Final Model

Latent Variable	Indicators	Item Loadings	Indicator Reliability (Item communality)	Higher Order Construct Reliability (outer loadings)	Composite Reliability	AVE	Discriminant Validity
OK	OK5	0.8120	0.6593		0.7649	0.5261	Yes
	OK7	0.7769	0.6036				
	OK9	0.5616	0.3154				
SK	SK1	0.8098	0.6558		0.9106	0.7729	Yes
	SK2	0.9252	0.8560				
	SK3	0.8983	0.8069				
CFIP					0.9443	0.5911	
C	C2	0.8271	0.6841	0.6836	0.8948	0.7396	Yes
	C3	0.9011	0.8120	0.7453			
	C4	0.8501	0.7227	0.7026			
IA	IA1	0.8957	0.8023	0.7191	0.9293	0.8142	Yes
	IA2	0.9123	0.8323	0.7425			
	IA3	0.8989	0.8080	0.7209			
USU	USU1	0.8440	0.7123	0.8211	0.9218	0.7466	Yes
	USU2	0.8643	0.7470	0.8380			
	USU3	0.8567	0.7339	0.8305			
	USU4	0.8906	0.7932	0.7561			
E	E2	0.9404	0.8844	0.8173	0.9600	0.8889	Yes
	E3	0.9469	0.8966	0.7876			
	E4	0.9412	0.8859	0.8088			
TP	TP1	0.8351	0.6974		0.9501	0.7606	Yes
	TP2	0.8704	0.7576				
	TP3	0.8733	0.7627				
	TP4	0.8932	0.7978				
	TP5	0.9044	0.8179				
	TP6	0.8544	0.7300				
TAM	TAM1	0.8604	0.7403		0.9597	0.7988	Yes
	TAM2	0.8866	0.7861				
	TAM3	0.9152	0.8376				
	TAM4	0.8987	0.8077				
	TAM5	0.9159	0.8389				
	TAM6	0.8843	0.7820				
TCC	TCC1	0.9067	0.8221		0.9751	0.8670	Yes
	TCC2	0.9395	0.8827				
	TCC3	0.9492	0.9010				
	TCC4	0.9284	0.8619				
	TCC5	0.9364	0.8768				
	TCC6	0.9260	0.8575				
BL	BL1	0.7406	0.5485		0.8498	0.5318	Yes
	BL2	0.7816	0.6109				
	BL4	0.6877	0.4729				
	BL6	0.7652	0.5855				
	BL10	0.6640	0.4409				
BP	BP1	0.6134	0.3763		0.8819	0.5177	Yes
	BP2	0.7049	0.4969				
	BP6	0.7491	0.5612				
	BP7	0.8041	0.6466				
	BP8	0.7533	0.5675				
	BP9	0.7172	0.5144				
	BP10	0.6793	0.4614				

constructs must be discriminant from each other and the higher order construct must be discriminant from the other separate constructs within the model. As the first order constructs of CFIP were discriminant from each other and CFIP was discriminant from the remaining model constructs, CFIP was determined to be a discriminant second order construct. The Fornell-Larcker criteria and cross loading comparison also revealed that all remaining constructs within the final model were discriminant.

Table 6.15 Fornell-Larcker Criteria for Final Model

(Shaded value on the diagonal represents √AVE)

	BL	BP	C	CFIP	E	IA	OK	SK	TAM	TCC	TP	USU
BL	0.729											
BP	0.582	0.720										
C	-0.194	-0.127	0.860									
CFIP	-0.156	-0.089	0.827	0.769								
E	-0.019	-0.033	0.508	0.772	0.943							
IA	-0.137	-0.057	0.691	0.920	0.620	0.902						
OK	-0.126	-0.049	0.161	0.217	0.071	0.253	0.725					
SK	0.224	0.227	-0.113	-0.099	-0.052	-0.050	0.076	0.879				
TAM	0.155	0.245	0.066	0.083	0.086	0.082	0.098	0.103	0.894			
TCC	-0.035	0.166	0.189	0.243	0.143	0.265	0.149	0.085	0.555	0.975		
TP	0.330	0.265	-0.113	-0.055	0.015	-0.035	-0.050	0.086	0.266	0.211	0.950	
USU	-0.180	-0.093	0.696	0.918	0.569	0.831	0.241	-0.123	0.057	0.229	-0.060	0.864

Table 6.16 Item Cross Loadings in Final Model

	BL	BP	C	CFIP	E	IA	OK	SK	TAM	TCC	TP	USU
CFIPC2	-0.1949	-0.0806	0.8271	0.6836	0.3946	0.5941	0.2109	-0.0575	0.1086	0.2822	-0.0574	0.5751
CFIPC3	-0.1843	-0.1609	0.9011	0.7453	0.4558	0.6199	0.1032	-0.1	0.0279	0.1491	-0.1157	0.6316
CFIPC4	-0.1206	-0.082	0.8501	0.7026	0.4578	0.5694	0.1046	-0.1326	0.0363	0.0612	-0.1152	0.5868
CFIPE2	-0.0182	-0.0269	0.4775	0.7191	0.9404	0.5743	0.0676	-0.033	0.0948	0.1556	0.0299	0.5234
CFIPE3	-0.0351	-0.036	0.4874	0.7425	0.9469	0.6076	0.084	-0.0483	0.0876	0.1567	0.007	0.5504
CFIPE4	-0.0014	-0.0304	0.4705	0.7209	0.9412	0.5704	0.0482	-0.0648	0.0614	0.0904	0.0044	0.5362
CFIPIA1	-0.1192	-0.0463	0.6213	0.8211	0.571	0.8957	0.24	-0.0413	0.0766	0.2232	-0.0258	0.7237
CFIPIA2	-0.1115	-0.058	0.6247	0.838	0.5623	0.9123	0.2465	-0.0222	0.0878	0.2601	-0.0286	0.762
CFIPIA3	-0.1412	-0.0511	0.6255	0.8305	0.5445	0.8989	0.1988	-0.0731	0.0567	0.2336	-0.0416	0.7648
CFIPUSU1	-0.164	-0.0661	0.5595	0.7561	0.4569	0.6834	0.2244	-0.0898	0.0571	0.178	-0.0524	0.844
CFIPUSU2	-0.1389	-0.0819	0.6327	0.8173	0.5588	0.7145	0.1812	-0.1201	0.0376	0.1843	-0.0583	0.8643
CFIPUSU3	-0.1397	-0.0805	0.6069	0.7876	0.4866	0.7091	0.1653	-0.1435	0.0749	0.204	-0.0415	0.8567
CFIPUSU4	-0.1816	-0.0906	0.6031	0.8088	0.4629	0.7651	0.2609	-0.0711	0.0277	0.2245	-0.0562	0.8905
OK5COR	-0.1136	-0.0377	0.1112	0.1364	0.0328	0.1618	0.812	0.0425	0.0894	0.1023	-0.058	0.1505
OK7COR	-0.0958	-0.0571	0.1589	0.2411	0.1141	0.2753	0.7769	0.053	0.0841	0.1561	-0.0001	0.2587
OK9COR	-0.0465	0.0054	0.067	0.0703	-0.0216	0.0872	0.5616	0.1025	0.0154	0.0449	-0.0648	0.0966
Q411BL4	0.6877	0.3526	-0.1165	-0.102	0.0069	-0.1074	-0.0786	0.1429	0.1219	-0.0645	0.2354	-0.1242
Q417BL6	0.7652	0.4648	-0.1801	-0.1677	-0.0855	-0.1189	-0.0785	0.2672	0.0662	-0.0151	0.2151	-0.1875
Q418BP6	0.4415	0.7491	-0.1043	-0.0769	-0.004	-0.0595	-0.0437	0.1905	0.1689	0.1358	0.2399	-0.0933
Q421BP7	0.3835	0.8041	-0.0752	-0.0478	-0.0179	-0.0127	-0.0264	0.2073	0.1524	0.132	0.206	-0.0596
Q424BP8	0.3668	0.7533	-0.0474	0.0224	0.018	0.0595	0.0452	0.1616	0.2132	0.2336	0.1683	0.0332
Q427BP9	0.354	0.7172	-0.0523	-0.0297	0.0221	-0.0194	-0.0364	0.1051	0.1963	0.1147	0.1715	-0.0484
Q429BL10	0.664	0.4161	-0.1155	-0.0812	-0.0004	-0.0635	-0.0588	0.1269	0.1283	0.0345	0.2815	-0.097
Q42BL1	0.7406	0.4037	-0.1411	-0.1021	0.0028	-0.1005	-0.1044	0.1564	0.1133	-0.0281	0.2245	-0.1103
Q430BP10	0.4441	0.6793	-0.1112	-0.0902	-0.0557	-0.0633	-0.0156	0.1793	0.1576	0.1409	0.2174	-0.0841
Q43BP1	0.3987	0.6134	-0.104	-0.0954	-0.053	-0.0909	-0.1008	0.1303	0.1951	0.0849	0.1841	-0.083
Q45BL2	0.7816	0.4714	-0.1461	-0.1103	0.0147	-0.1092	-0.1358	0.1121	0.1408	-0.0563	0.2513	-0.1315
Q46BP2	0.5001	0.7049	-0.1251	-0.1094	-0.0604	-0.0823	-0.0617	0.1579	0.1525	0.0114	0.1413	-0.1098
Q5TP1	0.2637	0.2231	-0.0594	-0.0231	0.0119	-0.0103	-0.0231	0.1139	0.1818	0.2177	0.8351	-0.0248
Q5TP2	0.2834	0.2304	-0.0427	-0.0123	0.0077	0.0111	0.0017	0.0995	0.2036	0.1937	0.8704	-0.0205
Q5TP3	0.2973	0.2548	-0.1019	-0.0499	0.0258	-0.0313	-0.0654	0.0972	0.214	0.1484	0.8733	-0.0644
Q5TP4	0.2985	0.2295	-0.1096	-0.0568	0.0089	-0.0385	-0.0199	0.0674	0.2568	0.1877	0.8932	-0.0601
Q5TP5	0.2984	0.241	-0.1213	-0.08	-0.0135	-0.0601	-0.0346	0.0472	0.2478	0.2046	0.9044	-0.0827
Q5TP6	0.2845	0.2092	-0.1416	-0.0591	0.0351	-0.0483	-0.1126	0.0383	0.2737	0.1593	0.8544	-0.056
Q6TAM1	0.1318	0.2222	0.039	0.0717	0.0987	0.0632	0.0462	0.0602	0.8604	0.4696	0.2479	0.0495
Q6TAM2	0.1014	0.205	0.0931	0.0954	0.0653	0.1007	0.1206	0.1129	0.8866	0.5083	0.2121	0.0732
Q6TAM3	0.1482	0.2311	0.0838	0.1025	0.0879	0.1102	0.1096	0.1027	0.9152	0.5322	0.2349	0.0748
Q6TAM4	0.1717	0.2155	0.071	0.0804	0.0727	0.0769	0.099	0.0802	0.8987	0.4874	0.2473	0.0603
Q6TAM5	0.1267	0.2167	0.0697	0.075	0.0791	0.0684	0.0707	0.089	0.9159	0.4966	0.2359	0.048
Q6TAM6	0.1507	0.2203	-0.0074	0.0167	0.0586	0.0152	0.0779	0.1047	0.8843	0.4784	0.2472	-0.0043
Q7TCC1	-0.0688	0.1391	0.1632	0.2348	0.1343	0.2621	0.1622	0.0515	0.4839	0.9067	0.2169	0.2335
Q7TCC2	-0.0262	0.1669	0.1968	0.2363	0.1284	0.2638	0.1618	0.0899	0.5164	0.9395	0.1843	0.2177
Q7TCC3	-0.0334	0.1411	0.2117	0.2584	0.1479	0.278	0.1619	0.065	0.5259	0.9492	0.1897	0.2436
Q7TCC4	-0.0132	0.1526	0.1805	0.2327	0.1371	0.2593	0.1185	0.0891	0.5277	0.9284	0.1882	0.2159
Q7TCC5	-0.0189	0.1778	0.1506	0.1949	0.1234	0.2058	0.1138	0.0947	0.533	0.9364	0.2116	0.1842
Q7TCC6	-0.0355	0.1464	0.1535	0.199	0.1254	0.2128	0.1149	0.0815	0.5107	0.926	0.1908	0.1864
Q8SK1	0.1367	0.1577	-0.1246	-0.1164	-0.0827	-0.0629	0.0781	0.8098	0.0539	0.0577	0.0073	-0.1292
Q8SK2	0.2014	0.2015	-0.0855	-0.0665	-0.039	-0.0226	0.1068	0.9252	0.0818	0.0758	0.05	-0.0811
Q8SK3	0.234	0.2286	-0.0967	-0.0887	-0.028	-0.0521	0.0261	0.8983	0.1225	0.0854	0.1436	-0.1199

Given the results shown in Tables 6.14, 6.15 and 6.16, changes to the original measurement model were justified. Accordingly, the changes made have been addressed next.

The latent constructs of SK and the trust constructs of TP, TAM, TCC remained intact. The new OK construct retained only 3 three items – OK5, OK7 and OK9. The CFIP construct required only minor, but noteworthy, adjustments as well. One manifest item (C1) from the CFIP Collection dimension was deleted due to showing an outer loading of only 0.5323 on the higher order CFIP construct in the last re-test of the model. As CFIP was not an exploratory construct and dropping the manifest variable did not adversely affect AVE of CFIP, this was deemed to be an acceptable adjustment. Similarly, one manifest item (E1) from the CFIP Error dimension was dropped due to its outer loading of 0.6003.

Consistent with expectations of an exploratory construct such as OSN CPM, substantial changes (administered gradually) were required to the construct. The end result was that the Boundary Ownership dimension was dropped entirely because outer loadings of manifest variables on the construct remained poor and AVE of BO did not improve to an acceptable level.

Secondly, OSN CPM was determined to be a first order construct. Even with only two dimensions (BL and BP), the highest AVE of OSN CPM achieved was 0.3959, well below the critical criteria of .50. Thus it became obvious that OSN CPM as measured was not a second order construct as hypothesised.

Several manifest variables associated with BL and BP were also trimmed from the model. Due to the exploratory nature of the OSN CPM construct, more liberal acceptance criteria were employed in determining item retention. Given that OSN CPM was a defined latent construct, conservative item loading thresholds in excess of 0.70 would normally be required to assess indicator reliability. However, as the construct was modified from a different context (blogging), the original scale included items with low factor loadings (Child, Pearson and Petronio, 2009), and untested items generated via focus group were included in this test, the more liberal cut-off of 0.6 was justified as it fell at the conservative end of Hair, Ringle and Starstedt's (2013) acceptable range. In addition, Hair et al (2010) suggested that items with loadings between 0.4 and 0.7 only be dropped when improvements to AVE have been realized. Using these modified criteria, the final measurement model was comprised of 5 items for BL (BL1, BL2, BL4, BL6, BL10) and 7 items for BP (BP1, BP2, BP6, BP7, BP8, BP9, BP10).

The five BL items retained included BL1, BL2, BL4, BL6, BL10. Specifically, four of the six items from the original Boundary Linkage scale proposed by Child, Pearson and Petronio (2009) (BL1, BL2, BL4, BL6) were retained whereas only one of the items proposed by the focus group in this Project was retained (BL10). The resultant BL measure exhibited acceptable composite reliability (CR = 0.8498), convergent validity (AVE = 0.5318) and discriminant validity (Table 6.15 and 6.16). Seven BP items were retained including BP1, BP2, BP6, BP7, BP8, BP9, BP10, three of which originated in Child, Pearson and Petronio (2009) (BP 1, BP2, and BP6) and four of which were developed for this Project (BP7, BP8, BP9 and BP10). The resultant BP measure also exhibited acceptable measurement reliability and validity (CR = 0.8819; AVE = 0.5177; Table 6.15 and 6.16).

Another important change to the model was the transition of TP, TCC and CFIP to exogenous variables. As a result of poor levels of R^2 for the hypothesised endogenous location of trust and CFIP constructs, the exploratory nature of this investigation and support within the literature, TP, TCC and CFIP were made exogenous constructs to predict OSN CPM.

Structural Model

The structural model represents the structural relationships, or paths, between the measurement constructs (Hair et al, 2010). In PLS-SEM, evaluation of the structural model permits determination of dependence relationships between constructs in order to draw causal inferences. Typically, structural equation modelling (SEM) can assess one criterion for causation – covariance – via statistically significant path relationships. However, SEM itself does not enable confirmation of causation.

Causal inferences can only be confidently established when three other criteria of causation are present – sequence, nonspurious covariance and theoretical support (Hair et al, 2010). Theoretical support can only be offered by the researcher and efforts to substantiate findings based upon theory have been included in the Chapter 7. However, neither sequence nor nonspurious covariance could be established with this analysis. As this Project utilised a cross-sectional survey, sequence could not be established as it may be in instances where longitudinal or experimental designs have been employed. And, while nonspurious covariance relationships can be tested when covariance based SEM (CB-SEM) techniques are employed, PLS-SEM does not enable such comparisons because path relationships are calculated independent of the other model constructs. Thus, paths relationships in this research have been evaluated to draw conclusions about dependence relationships among a variety of previously untested constructs within the conceptual model, but conclusions about causation were not made. Instead, the exploratory nature of this research emphasised model development via the identification of dependence relationships may also be assessed.

Path Coefficients

The strength of construct relationships was calculated using the SmartPLS bootstrapping algorithm with cases equal to 835 (equal to the sample size), 5000 samples and no sign changes specified. Results produced standardised path coefficients and significance indicators via empirical t values. Table 6.17 presents these output measures along with significance calculations (critical t value and p value). The strongest relationships in the final model were detected in the paths from BL to BP (path coefficient = 0.538), TCC to TAM (path coefficient = 0.522), TP to BL (path coefficient = 0.303) and SK to BL (path coefficient = 0.196). OK negatively influenced to BL at a level of significance of p=0.001. CFIP also negatively influenced BL at a significance level p<0.01.

Table 6.17 Bootstrapping Results of Final Model

Path	Standardised Path Coefficient	Empirical t value	Critical t value	p value
BL -> BP	0.538	18.467	***	0.000
CFIP -> BL	-0.098	2.605	**	0.009
CFIP -> C	0.827	42.273	***	0.000
CFIP -> E	0.772	38.394	***	0.000
CFIP -> IA	0.920	123.852	***	0.000
CFIP -> USU	0.918	110.128	***	0.000
OK -> BL	-0.104	3.234	**	0.001
SK -> BL	0.196	6.148	***	0.000
SK -> BP	0.091	3.023	**	0.003
TAM -> BP	0.152	5.405	***	0.000
TCC -> TAM	0.522	18.268	***	0.000
TP -> BL	0.303	9.097	***	0.000
TP -> TAM	0.155	4.466	***	0.000

*p<.05; **p<.01, ***p<.001

Total Effects

Total effects of one construct on another must be calculated when there are both direct and indirect effects upon a construct via a mediating construct. In the case of the final model, all five exogenous constructs contributed to BP via a mediating construct. Two constructs' effect was mediated by TAM (TP and TCC) and four constructs' effect upon BP were mediated by BL. SK was the only exogenous construct with a direct effect on BP.

Table 6.16 presents the total effects of exogenous constructs on the dependent construct BP calculated as the product of the indirect path coefficients plus the path coefficient of the direct path. From this table it is apparent that one's trust in close connections and trust in OSN provider have large effects on BP (0.281 and .187 respectively) with the majority of TP's indirect effect on BP being derived via the BL mediator. Although SK has a small but significant direct on BP (0.91), its total effect is much greater (0.196). Both OK and CFIP contribute little effect to BP, but the negative direction of the effect must be noted.

Table 6.18 Total Effects of all constructs on BP

	Direct Effects	Indirect effects	Indirect effects	Total effects
		(BL mediator)	(TAM mediator)	BP
SK --> BP	0.091	0.105	0.000	0.196
OK --> BP	0.000	-0.056	0.000	-0.056
CFIP --> BP	0.000	-0.053	0.000	-0.053
TP --> BP	0.000	0.163	0.024	0.187
TCC --> BP	0.000	0.000	0.281	0.281

Coefficient of Determination (R^2)

In addition to path weights and significance, it is important to examine how much variance within the endogenous construct is explained by the predicting constructs. This is done via examination of the coefficient of determination (R^2). While appropriate levels of R^2 depend upon the context of the study, some recommend minimum values of 0.10 are required (Falk and Miller 1992) and others suggest that values of 0.20 are considered high in the context of consumer behaviour (Hair et al 2013). The final model presented in Figure 6.2 shows that the exogenous constructs of OK, SK, CFIP and TP account for 17.2 per cent ($R^2 = 0.172$) of the variance in Boundary Linkages (BL) and SK, BL, and the trust constructs account for 37.1 per cent of the variance in Boundary Permeability (BP). As this is an investigation of OSN consumer behaviour and both values are well above a recommended minimum or 0.10 and the lowest value is approaching a recognised 'high' value in consumer behaviour construct, these values were determined to be acceptable.

As the goal of most PLS research is to arrive at the most parsimonious model, the effect size (f^2) of each exogenous construct must be established as well. To do this, the coefficient of determination (R^2) is calculated for the endogenous construct using the PLS algorithm in Smart PLS when the exogenous construct is included in the model and again when it is excluded. Effect sizes (f^2) are thought to be weak when $f^2 = 0.02$, moderate when $f^2 = 0.15$ and high when $f^2 = 0.35$.

Table 6.18 shows the effect size of each exogenous construct in the final model. These results show that OK ($f^2 = 0.012$) and CFIP ($f^2 = 0.011$) have little effect on BL while SK ($f^2 = 0.045$) has a weak effect on BL. TP ($f^2 = 0.109$) also has a weak effect on BL, but its effect is much larger than that of SK. Further, TCC has a strong effect on TAM ($f^2 = 0.389$) while TP has a weak effect on TAM ($f^2 = 0.034$). No exogenous variable has a substantial effect on BP.

Table 6.19 Effect size (f^2) of exogenous constructs

	BL R^2			BP R2			TAM R2		
	included	excluded	f^2	included	excluded	f^2	included	excluded	f^2
SK	0.172	0.135	0.045	0.371	0.364	0.011	n/a	n/a	n/a
OK	0.172	0.162	0.012	0.371	0.371	0.000	n/a	n/a	n/a
CFIP	0.172	0.163	0.011	0.371	0.371	0.000	n/a	n/a	n/a
TP	0.172	0.082	0.109	0.371	0.372	-0.002	0.331	0.308	0.034
TCC	n/a	n/a	n/a	0.371	0.371	0.000	0.331	0.071	0.389

In all, the final model was effective at explaining Boundary Permeability ($R^2 = 0.371$). Not only was the relationship between boundary linkage and boundary permeability the most significant revealed in the model, it was also determined that BL had the largest effect on BP among all predictive constructs. In addition to the dependence relationship between BL and BP, SK (β = 0.091, $p < 0.01$) and TAM (β = 0.152, $p < 0.001$) also influenced BP directly.

All exogenous constructs in the final model showed mediated relationships with the extent of information sharing on OSNs (BP) as well. When total effects were analysed (Table 6.18), it was revealed that TCC (total effects = 0.281), SK (total effects = 0.196), and TP (total effects = 0.187) had the strongest effect on BP. Weak and negative total effects were also observed for OK (total effects = -0.056) and CFIP (total effects = -0.053). However, examination of effect size (Table 6.19) revealed that each of the effects on BP contributed by exogenous constructs was not important in explaining the variance in the construct. Instead, the exogenous constructs explained communication privacy management via the greater effect sizes observed upon the mediating constructs of boundary linkages and trust in all members.

A sizable amount of the variance in BL ($R^2 = .172$) was explained by the exogenous constructs tested in the model. Privacy concern (CFIP) and objective knowledge (OK) were negatively and significantly related to BL whereas SK and TP were positively and significantly related to BL. Specifically, the dependence relationship between CFIP and BL was reasonably strong (β = -0.098, $p < 0.01$) but little effect was observed ($f^2 – 0.011$). Similarly, the dependence relationship between OK and BL was adequate (β = -0.104, $p < 0.05$), but negligible effect size on BL was revealed ($f^2 = 0.012$). Subjective Knowledge (SK) had significant direct dependence with BL (β = 0.196, $p < 0.001$) but a weak effect ($f^2 = 0.045$). The dependence between TP and BL was strongest ($\beta = 0.303$, $p < 0.001$), as was the effect size the largest ($f^2 = 0.109$), but the effect size was still classified as weak (Hair et al, 2013).

A large portion of the variance in TAM ($R^2 = .331$) was explained by the other trust variables (TP and TCC). Specifically, TP was directly and significantly dependent with TAM ($\beta = 0.155$, $p < 0.001$) but only a weak effect was detected in the relationship (f2 = 0.034) whereas TCC had a much stronger relationship ($\beta = 0.522$, $p < 0.001$) with strong effects on TAM ($f^2 = 0.389$).

In conclusion, the statistical results of the measurement model presented in this section have resulted in the final model (Figure 6.2) being offered as a valid and reliable measurement of each of the constructs under study within the unique context of OSNs. The statistical results presented for the path structure and effects of the relationships between constructs provided evidence that the final model represented an appropriate understanding of the relationships within the model. As a result, some of the hypothesised relationships in this Project were supported and others were not. The results also indicated that unexpected relationships emerged. Therefore, the empirical evidence presented in this Chapter provided material for interpretation and discussion. As such, Chapter 7 will examine the important conclusions and their possible meanings.

7 Discussion

The purpose of this research was to extend the privacy literature by investigating additional explanations of the privacy paradox within online social networks, thereby providing additional understanding of information disclosure decisions in these environments. There were four specific research objectives derived from this intent. Namely, this research sought: i) to validate a prominent conceptualization of privacy concern in the context of online social networks, ii) to explain personal information disclosure in online social networks using Communication Privacy Management theory, iii) to explain the role of privacy literacy in influencing online social network information disclosure decisions, and iv) to establish the role of trust in consumer information disclosure behaviours in online social networks. Each of these objectives was accomplished with this Project, though the conceptual model as hypothesised was not fully supported.

Consistent with the objectives of this Project which entailed investigation of previously untested relationships in the privacy calculus in online social networks (OSNs), a model development strategy (Hair et al, 2010) was employed. In contrast to a confirmatory modelling strategy wherein a theorised model is accepted or rejected or a competing models strategy wherein more than one theorised model is presented and tested, this research entailed presentation of a theoretically grounded model as a starting point. However, given statistical results of the conceptual model and guided by theory, that model had to be re-specified. Model re-specification is a commonly accepted approach so long as theory guides the process and the "purpose of the modelling effort is to improve the framework through modifications of the structural or measurement models" (Hair et al, 2010, p. 629).

Analysis of the hypothesised conceptual model herein indicated that modification to both the measurement and structural models was required. Thus, the results achieved will be discussed in two ways. The measurement model, or the constructs under investigation, will first be discussed in Section 7.1 in order to highlight the re-specification of constructs required. Section 7.2 will provide a discussion of the structural model, or the causal paths revealed from statistical tests. Results of the hypothesised structural relationships are discussed first followed by a discussion of the final model realised after re-specification.

7.1 Measurement Model

Before discussing the relationships within the model, a necessary first step was to examine the measurement reliability and validity of constructs within the model. This approach is common in any study utilising a structural equation model analysis, but is particularly important in models incorporating new or revised measurement instruments. Given the lack of consistent acceptance of a definition for privacy concern established in Chapter 3, the nascent empirical application of Communication Privacy Management and the originality of the objective knowledge scale, the obligation to discuss the measurement model in depth was acute.

In covariance-based structural equation model (CB-SEM) analyses, Confirmatory Factor Analysis (CFA) is typically used to test the measurement model (Hair et al, 2010); however, in partial least squares structural equation models (PLS-

SEM) using reflective measures as was the case herein, the measurement model was assessed via outer loadings, composite reliability, convergent validity and discriminant validity measures consistent with the literature (Hair et al, 2013). Using recommended values for determining reliability and validity (Hair et al 2010; 2013) as presented in Chapter 6, the final measurement model was ultimately concluded to be both reliable and valid. Yet, to arrive at the final model modification of the original measurement model was required. Consequently, results of the measurement model yielded some interesting findings which have been discussed in Sections 7.1.1 through 7.1.4.

7.1.1 Concern for Information Privacy (CFIP) in OSN Contexts

The literature review presented inconsistent views of privacy and even in instances where privacy definitions had been narrowly constrained to represent consumer information privacy concern, different operationalizations of the construct were employed. However, despite a lack of universal acceptance for one privacy concern conceptualisation, the concern for information privacy (CFIP) construct suggested by Smith, Milberg and Burke (1996) had been commonly used, confirmed in a number of contexts including online (Bellman et al, 2004; Van Slyke et al, 2006) subsequent offline tests (Stewart and Segars, 2002) and with a sample of New Zealanders (Rose, 2005) and had provided the basis for other privacy scales (i.e., Xu et al, 2008; 2011). But, the support for the CFIP construct uncovered in the literature did not mean that the construct could be assumed to be appropriate in the context of OSNs because the contextual nature of privacy was consistently espoused (i.e., Westin 1967; Goodwin, 1991) and CFIP had not been previously tested in these environments. Similarly, CFIP could not be assumed to be appropriate in a Canadian context as it had never been tested in that culturally distinct (Adams, 2003) environment despite claims that privacy was culturally relative (Westin, 1967; Moore, 2003). Finally, as Hair et al (2010) stated, "evidence of model stability and generalizability can only come from performing the analysis on additional samples and contexts" (p.680), a test of the CFIP construct for the context of OSNs and Canadian users was necessary and thus formed the basis of the first objective of this study - to validate a prominent conceptualization of privacy concern in the context of online social networks.

In spite of uncertainty over the validity of concern for information privacy (CFIP) measure in the unique context of this study, results of the measurement model analysis served to validate the CFIP construct in this new context and therefore the first objective of this research – to validate CFIP in a new context - was accomplished. Specifically, the results of this research support the treatment of CFIP as a multidimensional construct comprised of each of the four dimensions originally proposed by Smith, Milberg and Burke (1996) – collection, improper access, unauthorized secondary use and errors. Consequently, these results provided additional support for the ability of the CFIP measure to appropriately represent privacy concern. When combined with the results from other studies offering external validation of the construct (Stewart and Segars, 2002; Bellman et al, 2004; Rose, 2005; Van Slyke et al, 2006), a compelling argument has begun to be built for the universal applicability of this measure.

Furthermore, results supported CFIP could be effectively represented as a second order construct in the context of this Project as had been suggested by Stewart and Segars (2002). Each of the first order dimensions of CFIP were associated with the higher order CFIP latent construct with strong, statistically significant paths ($\beta = 0.727$ to $\beta = 0.920$, $p < 0.000$) and CFIP exhibited both convergent (Table 6.14) and discriminant validity (Tables 6.15 and 6.16). The hierarchical structure of the construct revealed means that information privacy concern may be thought of as consisting of reducible elements as argued by reductionists (i.e., Thomson, 1975; Posner, 1981), although each of those elements reflect one grand overarching concept as argued by coherentists (i.e. Schwartz, 1968; Parent, 1983). As such, information privacy concern is not singularly a concern over information collection or concern over improper access or concern over unauthorised secondary use or concern over errors, but a collection of each of those concerns.

However, some caution must be exercised in generalising too widely from these results. While assessments of item and construct reliability and validity are appropriate measurement model assessments within a PLS-SEM analysis and serve the purpose of supporting the first objective of this Project, the results have not been calculated identically to more familiar confirmatory factor analysis techniques within CB-SEM software. Confirmatory techniques have revealed similar conclusions about construct structure (Tenenhaus, 2008), but they are not the same thing and therefore conclusions cannot be used in the same way (Hair, Ringle and Starstedt, 2011). Thus, where the measurement model findings suggested a slightly more parsimonious CFIP scale with 13 manifest variables (three items for each dimension of collection, improper access and errors and four items for unauthorised secondary use) this research has not argued this to be a definitive measurement scale. Instead, findings permitted the conclusion that CFIP comprised of four distinct dimensions had been validated, but use of a confirmatory technique in this context would be required to confidently advocate for the marginally more parsimonious scale revealed.

In addition, the results did also suggest that there may be redundancy within the scale measuring the CFIP Error dimension as evidenced a high composite reliability value (CR = 0.9600). Consequently, an additional opportunity to explore a more parsimonious scale in future research was identified although such an action will be accompanied by the risk of construct underidentification that results when the number of manifest variables is less than three (Hair et al, 2010). Therefore, researchers employing CFIP must be mindful of the balance between redundancy and underidentification risks associated with the construct.

7.1.2 Communication Privacy Management

Based upon the work of Child, Pearson and Petronio (2009), OSN Communication Privacy Management (CPM) coordination processes were hypothesised as a second order construct with three dimensions – Boundary Ownership (BO), Boundary Linkages (BL) and Boundary Permeability (BP). Interestingly, the hypothesised structure of this construct was not supported by the requisite statistical tests, yet a reliable and valid measure of the construct did emerge. There were three particularly intriguing findings with respect to the OSN CPM construct revealed through the analysis of the measurement model. Specifically, the hypothesised boundary ownership dimension was not detected; reliable and valid measures of boundary linkages and boundary permeability emerged that demonstrated the importance of context in decision rules; and remaining dimensions of OSN CPM were shown to be first order factors rather than the hypothesised hierarchical structure.

The inability to retain the Boundary Ownership dimension of OSN CPM within the measurement model was somewhat surprising, though not entirely unexpected after review of pilot test results. Recall that results evaluated at the pilot test stage of the research design suggested that internal reliability of Boundary Ownership was not established (see Tables 5.9 and 5.10), but the measure was retained for analysis with data from the full sample. Results of the full sample confirmed that the Boundary Ownership measure failed to achieve internal consistency (CR = 0.1449), indicator reliability among BO manifest variables was poor, convergent validity was well below established criteria (AVE = 0.1315) and discriminant validity was not observed (Table 6.13). Thus, this comprehensive assessment of measurement model test statistics supported indications from the pilot test that the BO dimension was not reliable as measured.

Even though Boundary Ownership was not detected within the measurement model, the results could not be interpreted to suggest that Boundary Ownership does not factor into CPM in OSNs. Rather, results conclusively indicated that the BO dimension has not been measured appropriately. More specifically, the original BO items offered in Child, Pearson and Petronio's (2009) Blogging Privacy Management Measure (BPMM) did not translate to the context of OSNs and the items generated from a focus group of peer experts similarly failed to capture the essence of

Boundary Ownership in OSNs. Although unexpected at the outset of the research, the lack of Boundary Ownership evidenced in the results constituted an interesting finding that provides an opportunity for future research to attempt more rigorous development of this dimension.

However, the conclusion that Boundary Ownership had not been sufficiently captured by the manifest items developed for a blogging context appeared to indicate that boundary ownership rules about personal information could be different within online social networks compared to other contexts. The claim that individuals' information privacy related behaviour may be dependent upon context has certainly been substantiated within the literature (i.e., Xu et al, 2011; Christofides, Muise and Desmarais, 2009). And, since privacy was shown to be contextual (i.e. Goodwin, 1991; Westin, 1967), then the way individuals manage their privacy could logically differ by context. Indeed, Child and Petronio (2011) argued generally that context could act as a catalyst for changing personal or collectively held privacy rules because of a need to reach a particular goal and specifically identified that the OSN Facebook provided a unique set of contextual constraints. Therefore, as OSN environments primarily exist to facilitate information sharing and re-sharing to achieve social capital benefits, it is possible that individuals erect boundaries around information co-owned by their intended audiences and unintended audiences of silent listeners differently than in other online contexts such as blogs. Thus, future research should attempt to investigate Boundary Ownership in OSNs in greater detail in order to understand how individuals navigate the information decisions in environments where personal information becomes co-owned by, or at least accessible to, numerous parties including one’s direct connections, friends-of-friends, the OSN provider, third party advertisers and the general public.

From the final measurement model the resultant operationalization of Boundary Linkages and Boundary Permeability constituted a major contribution of this Project as tests of this kind did not exist in the literature. Measurement model results revealed that Boundary Linkages and Boundary Permeability were appropriately measured but could be expressed more parsimoniously than the twenty-four manifest items used (12 for each dimension). Importantly, the retained indicators of Boundary Linkages and Boundary Permeability (Table 7.1) were shown to be a combination of the original items suggested by Child, Pearson and Petronio (2009) for Blogging Privacy Management and those developed specifically for this Project through focus group peer expert consultation. It appeared from the results that boundary linkage behaviours in OSNs were similar to those within the context of blogging as four of the five retained items in the measure were original to the Child, Pearson and Petronio (2009) scale. Conversely, only half of the original boundary permeability behaviours were retained from the original scale and the final measurement model for BP was supplemented by boundary permeability behaviours recommended by the focus group. The differences observed in operationalization of these two dimensions of OSN CPM suggested that similar to findings about boundary ownership and consistent with Child and Petronio’s (2011) assertion, context did alter privacy management rules but more so for the breadth and depth of information shared (boundary permeability).

Table 7.1 OSN Communication Privacy Management Measurement

Construct	Code	Item	Item Loading
Boundary Linkages	BL1	I have created a detailed profile so that others can link to me with similar interests.	0.7406
	BL2	I try to let people know my best activities and interests so I can find friends.	0.7816
	BL4	I comment on or like things on friends' pages to have others check out my profile.	0.6877
	BL6	I like to link to interesting websites to increase traffic on my profile.	0.7652
	BL10	I like to add 'applications' to improve my experience.	0.6640
Boundary Permeability	BP1	When I face challenges in my personal life, I feel comfortable talking about them.	0.6134
	BP2	I like my status updates or posts to be long and detailed.	0.7049
	BP6	I update my profile frequently.	0.7491
	BP7	I update my status frequently.	0.8041
	BP8	When something positive happens to me, I post about it.	0.7533
	BP9	My status updates generally indicate how I am feeling.	0.7172
	BP10	I like to provide detailed comments on friends' pages.	0.6793

One last observation about the OSN CPM measurement was also recognised as important. Contrary to the hypothesised structure of OSN CPM as a second order construct, results indicated that the measure was more appropriately expressed as first order due to the lack of discriminant validity of the higher order construct from other constructs within the model. While Boundary Linkages and Boundary Permeability were distinct from each other and all other constructs in the model, the same claim could not be made for OSN CPM. Thus, rather than be considered as parts of a larger whole, the first order nature of the construct suggested that the constructs were independent, though related.

However, just as the measurement model assessment provided for CFIP could not be treated as confirmatory results (Hair, Ringle and Starstedt, 2013), neither can these OSN CPM results be regarded as conclusive evidence of factor structure. The measurement reliability and validity assessed for Boundary Linkages and Boundary Permeability enabled the conclusion that the retained manifest items were appropriate in this specific path model, but confirmatory tests will be required in future research. The measurement model results therefore offered value as they constitute a starting point for testing the operationalization of the constructs. Where context has been recognized as critical in privacy research and no test of this kind had previously been undertaken in the context of OSNs, the evidence of empirical structure of CPM offered herein constituted a unique contribution of this research to the academic understanding of privacy management.

7.1.3 Privacy Literacy

Results of the privacy literacy measurement model statistics revealed some interesting insights with respect to how the accuracy of one's privacy knowledge could be appropriately measured. Privacy literacy was measured in two distinct ways – via a succinct three item pre-existing subjective knowledge scale intended to reflect an individual's confidence in their privacy knowledge and a newly developed ten item objective knowledge test meant to assess one's accuracy of privacy knowledge. Results of measurement model statistics for subjective knowledge (SK) suggested that the construct, as hypothesised, was psychometrically sound. Thus, these results served to validate the SK scale in the context of OSNs. In contrast, results of measurement model statistics for objective knowledge (OK) suggested that the construct, as hypothesised, was not acceptable.

While there was support for administering a true/false instrument about the topic of interest to indicate objective knowledge (i.e. Carlson, Bearden and Hardesty, 2007), there was no instrument available within the literature that specifically measured objective knowledge about privacy. Therefore, an objective knowledge instrument was selected from quiz questions posited on the website of the Office of the Privacy Commissioner of Canada. Given that this was a new scale with no objective tests to support its reliability or validity, it was not surprising that all items were not acceptable for the resultant construct measurement. From the hypothesised ten item scale, seven items were dropped as a result of poor indicator reliability and consideration for implications to the AVE statistic for the construct. The remaining three items within the Objective Knowledge measure are shown in Table 7.2. Overall, these items produced a reliable and valid measure of the OK construct as determined by acceptable composite reliability (CR = 0.7649), convergent validity (AVE = 0.5261) and discriminant validity (Table 6.15).

Table 7.2 Objective Knowledge Measurement

Code	Item	Item Loading
OK5	All Canadian organizations can collect your Social Insurance Number so they can identify you. **(False)**	0.8120
OK7	A privacy breach has occurred when there is unauthorized access to, or collection, use, or disclosure of personal information. **(True)**	0.7769
OK9	Under certain circumstances, an organization can disclose their customer's personal information to law enforcement officials without their customer's consent. **(True)**	0.5616

Identification and validation of an acceptable Objective Knowledge measure for privacy in OSNs was another important contribution of this research, but a few points must be clarified. First, similar to observations for Boundary Permeability and Boundary Linkage measurement models, the soft-modelling approach of PLS analysis did not permit conclusive confirmatory statements about factor structure. Second, the three retained items were indicative of privacy knowledge that was very commonly known and although effectively represented objective knowledge in a statistical capacity, may not have demonstrated any real depth of privacy knowledge. The ten-item hypothesised measurement instrument for OK included items of varying degrees of complexity that were intended to provide a comprehensive picture about what one accurately knows about privacy. Indeed, descriptive results of Objective Knowledge responses indicated that objective knowledge levels among the sample were collectively low. Thus, an OK measure that only represented common knowledge items may not effectively demonstrate the impact of poor objective knowledge on other items in the model.

So, while the three items retained for measurement of Objective Knowledge were appropriate in this context, other indicators of objective knowledge about privacy have not been precluded by results. Future research including an objective knowledge measure should explore ways in which this instrument may be improved. For example, in addition to assessing the reliability and validity of additional indicators, it would be beneficial to consider inclusion of Objective Knowledge as a manifest variable representing a summed test score or attempt to measure objective knowledge of other aspects of privacy relevant to OSNs. For instance, this scale reflected one's accuracy of knowledge about Canada's *Personal Information and Protection of Electronic Documents Act* (PIPEDA). Because PIPEDA is universal legislation applicable to all businesses collecting data within Canada and relies upon citizens self-reporting violations of the *Act*, it was justified that knowledge of the requirements of the Act and protections afforded under it were requirements of all citizens engaged in information exchange with businesses including OSNs and thus constituted a realistic measure. Further, in order to adequately effect control over personal information, one must be able to identify when violations, or boundary turbulence (Petronio, 2002), have occurred. However, there remain other aspects of privacy about which knowledge could also afford user control. Although PIPEDA was relevant to all Canadian Facebook users, the collectively low levels of objective knowledge about PIPEDA were notable and could perhaps be attributed to the distance of the regulations to the information exchange. Therefore, it would be interesting to investigate objective knowledge of the formal agreements users enter into with respective OSN providers (i.e. privacy policies) as the proximity of the agreement to the exchange might also impact information disclosure. Following this argument, alternate measurements of objective knowledge could be explored in future research, although the results of this research do offer support for measurement of objective knowledge according to legislation in countries where universal privacy legislation exists.

7.1.4 Trust

Three trust constructs were hypothesised in the measurement model – trust in the OSN provider (TP), trust in close connections (TCC) and trust in all members of an OSN (TAM). Both trust in the provider (TP) and trust in all members (TAM) had been used previously in the literature (Krasnova and Veltri, 2010). The trust in close connections (TCC) measure was identical to TAM, but the object of trust was modified. Although the instrument had not been administered previously with this object, the scale items had been validated as indicators of another trust object – OSN members.

Some important observations were made with respect to these trust measurement models. First, these tests showed that each of the trust measures were valid and distinct. Validation of TP and TAM served as reinforcement for pre-existing scales. Validation of the TCC measurement showed that trust in close connections was indeed distinct from other types of trust and therefore should continue to be measured in future research. The distinctiveness of these measures were consistent with indications from social capital research that there were different types of connections (i.e. Gronovetter, 1973; Sandefur and Laumann, 1998), or different levels of trust (Putnam, 2001) among connections and therefore indicated that trust in the different OSN stakeholder groups should be considered separately as hypothesised. Finally, the high composite reliability values (in excess of 0.95) for each trust measure suggested that there may have been redundancy issues in the scale. Therefore, future research should examine ways to achieve parsimony with these measures.

7.2 Structural Model

The structural model deals with the relationships among the constructs within the model. As this Project began with a hypothesised structure that was modified as a result of statistical results in conjunction with theoretical insight in the literature, the results of the structural model have been discussed according to the process undertaken. Despite the statistical evidence that the hypothesised model was insufficient, a number of important insights were revealed from those results that aided understanding of information privacy concern and information disclosure decisions in OSNs. Therefore, Section 7.2.1 has discussed findings revealed from the hypothesised structural model. As mentioned, model re-specification was required as a result of initial statistical results achieved in the analysis. Though re-specification was recognised from empirical evidence, re-specification had to also be driven by theoretical understanding of the relationships between constructs. Therefore, Section 7.2.2 has addressed the theoretical justification for model re-specification. Finally, insights drawn from the paths that emerged within the final re-specified model have been considered in Section 7.2.3.

7.2.1 Hypothesized model

There were four groups of hypotheses examined using statistical evidence presented in Chapter 6. Examination of the relationships as hypothesised was thought to add value to the discussion and aided in understanding how the structural model should be re-specified, therefore, the discussion of the hypothesised structural model that follows is based upon the statistical evidence derived from both the originally hypothesised model and the trimmed measurement model as detailed in Sections 7.1.1 through 7.1.4.

Privacy Literacy and Privacy Concern Relationships

The first group of hypothesised relationships within the structural model suggested that privacy literacy, conceptualised as objective and subjective knowledge, would reduce an individual's privacy concern in OSNs. Specifically, the following hypotheses were stated:

> H1: Subjective knowledge (SK) about privacy will influence OSN behaviour by reducing one's concern for information privacy (CFIP).
>
> H2: Objective Knowledge (OK) about privacy will influence OSN behaviour by reducing one's concern for information privacy CFIP.

Results of the hypothesised model revealed that there was indeed a negative and significant relationship between subjective knowledge and privacy concern ($\beta = -0.125$, $p < 0.001$), thus there was support for the first hypothesis. This result suggested that the confidence one has in their privacy knowledge can reduce privacy concern which was both intuitively logical and consistent with many similar relationships found in the literature. Specifically, individuals' confidence in 'privacy self-efficacy' (Rifon, LaRose and Lewis, 2007; Tow, Dell and Venable, 2010) or self-determined Internet literacy (Dinev and Hart, 2006c) was shown to have a negative association with privacy concern.

Results also revealed a significant relationship between objective knowledge and privacy concern, but it was not in the direction hypothesised. Whereas it was thought that one's objective knowledge about privacy would decrease one's concern for information privacy in OSNs, the opposite relationship was found ($\beta = 0.282$, $p < 0.001$). This was a particularly interesting observation as it offered some insight into a previously untested relationship. As there were no direct measures of objective knowledge of privacy in the literature, the hypothesised direction of this relationship was uncertain. Conclusions found in the literature suggested that greater Internet experience resulted in lessened privacy concern (Bellman et al, 2004; Dinev and Hart, 2006c) therefore it was reasoned that exposure to an environment afforded one the potential to acquire privacy knowledge accuracy (OK). However, the opposite relationship direction revealed in this analysis was more consistent with Moscardelli and Divine's (2007) findings that Internet experience was associated with higher privacy concern. Further, despite observing a negative relationship between Internet literacy and privacy concern, Dinev and Hart (2006c) suggested that the opposite relationship was also conceivable because technically literate individuals would have the ability to grasp the vulnerabilities of the Internet and therefore have stronger privacy concerns. Additional findings from Dinev and Hart's (2006c) study, suggested that awareness about more general topics ('social awareness') resulted in increased privacy concern. Although social awareness was not the same as objective knowledge as it was based on respondents' self-assessment, Dinev and Hart's conclusions about relationship between this type of awareness and privacy concern were congruous with the findings of this study – that the more one knows, the greater the privacy concern. Therefore, although the direction of the hypothesis (H2) was not supported, there have been indications in the literature that supported the finding.

Also, given the order of constructs presented in the hypothesised structural model, it appeared from results that the more one accurately knew about privacy caused greater privacy concern. Reasoning that someone with a better understanding about privacy would also possess a greater awareness of potential privacy risks, it is possible that increased knowledge creates justifiable privacy concern. However, it is essential to bear in mind that only dependence relationships could be determined using this research design and analytical technique. Thus, without conclusive determination of sequence, another likely interpretation of results could be that individuals with higher privacy concerns seek out more information about privacy and therefore might know more about the topic. However, given that descriptive results showed that privacy concern was collectively high and objective knowledge was collectively low within the sample this alternate explanation looked less likely. For, if high privacy concerns prompted greater information search and resultant knowledge about privacy issues we would have expected that objective knowledge scores would be consistently high. Further, the objective knowledge items that were retained as a result of measurement model trimming represented general and common knowledge about privacy but not the kind of information that respondents would necessarily have had to seek out in response to high privacy concerns.

In summary, what these results clearly showed was that accuracy of privacy knowledge and privacy concern were directly, significantly and positively related. While sequence could not be concluded from the empirical evidence, there were other clues within the data to suggest that the sequence of the relationship was more likely as that hypothesised. Specifically, results appeared to indicate that greater privacy knowledge accuracy leads to heightened privacy concern.

The dependence relationships revealed between objective privacy knowledge and privacy concern and between subjective privacy knowledge and privacy concern were thought to be important contributions of this research because empirical tests of privacy literacy such as this had not been found within the literature. The results supported claims that these relationships exist and were significant, but the results also showed that privacy literacy was not the only determinant of privacy concern ($R^2 = 0.091$). Consistent with the numerous antecedents of privacy concern identified by Xu et al (2008) and further evidenced in the literature review of the privacy calculus (Table 4.1), it was not expected that privacy literacy represented an exhaustive test of influences upon privacy concern. However, the finding that privacy literacy explained less than the minimum amount of variance (Falk and Miller, 1992) in privacy concern required to retain the relationship in the structural model meant that these relationships had to be re-specified. The significant findings did suggest that privacy literacy should be incorporated as an antecedent to privacy concern in future research attempting to provide a comprehensive understanding of influences on privacy concern.

Privacy Concern and Trust Relationships

The hypothesised relationships between CFIP and trust were not supported. The literature review indicated that trust was a direct outcome of privacy concern (Metzger, 2004; Malhotra, Kim and Agarwal, 2004; Milne and Culnan, 2004;

Eastlick, Lotz and Warrington, 2006; VanSlyke et al, 2006; Midha, 2012) and it was generally accepted that there was a negative relationship between these variables such that privacy concerns led to reduced trust.   Accordingly, hypotheses H3a, H3b and H3c stated that trust in the OSN provider (TP), trust in all OSN members (TAM) and trust in one's close connections (TCC) would all be negatively influenced by one's privacy concern.

Results of this research suggested that while there was a negative relationship between privacy concern and trust in the OSN provider, the relationship was not significant in the original structural model ($\beta = -0.052$, $p < 0.30$) and CFIP was found to be a very poor predictor of trust in the OSN provider (TP $R^2 = 0.003$). Thus, the results of this Project's analysis suggested that CFIP was not an antecedent to trust in the provider. Although the direction of the relationship was consistent with the literature suggesting that organisational trust was negatively impacted by privacy concern, the lack of significance revealed in this analysis might suggest a relationship between privacy concern and trust that could be closer to that revealed by Joinson et al (2010) and Lin and Liu (2012). Specifically, these authors separately revealed that trust moderated, rather than mediated, relationships between privacy concerns and information disclosure behaviours (Joinson et al, 2010) and that trust was a stronger predictor of disclosure behaviour than privacy concern (Lin and Liu, 2012). So, while trust in the OSN provider may still influence information disclosure behaviours, the hypothesis that trust in the provider overcame privacy concerns to enable disclosure was not supported by this study.

On the other hand, results of this study revealed significant relationships between CFIP and both trust in all members and trust in close connections as expected from H3b and H3c. But, rather than the negative relationship direction anticipated, the dependence relationship between CFIP and the interpersonal trust constructs (TAM, TCC) was positive. In particular, the positive influence of privacy concern on trust in close connections was quite strong and highly significant (β = 0.241, *p* < 0.001) whereas the influence of privacy concern on trust in all members was weak and less significant (β = 0.085, *p* < 0.05). Despite the evidence of significant relationships, privacy concern was a very poor predictor of both types of interpersonal trust (TCC R^2 = 0.058; TAM R^2 = 0.007).

Each of these findings was interesting because interpersonal trust relationships had not been previously tested in this manner. Most research that had incorporated trust into privacy calculus investigations had examined organisational trust as opposed to interpersonal trust (Metzger, 2004; Malhotra, Kim and Agarwal, 2004; Eastlick, Lotz and Warrington, 2005; VanSlyke et al, 2006; Midha, 2012). Among the few studies that isolated interpersonal trust (Dwyer, Hiltz and Passerini, 2007; Krasnova and Veltri, 2010; Krasnova et al, 2010[9]), connections with privacy concern were not empirically tested. While the hypotheses that interpersonal trust would reduce privacy concern (H3b, H3c) were not supported by this Project, the lack of relationships constituted interesting contributions of this research. Particularly, just as privacy concern failed to predict trust in the provider, results of this analysis revealed that privacy concern was not antecedent to interpersonal trust either, but these results do not suggest that interpersonal trust was an unimportant influence upon information disclosure behaviours in OSNs. Thus, consistent with

[9] Krasnova et al (2010) did find a negative, although non-significant, relationship between trust in OSN members and perceived privacy risk, but privacy concern was not measured.

Joinson et al's (2010) and Lin and Liu's (2012) observations that trust influenced disclosure behaviour but not through direct relationships with privacy concern, these results suggested that alternate locations of trust in the structural model needed to be explored.

Trust and Communication Privacy Management Relationships

The remaining research hypotheses involved the expected relationships between trust and OSN behaviours conceptualised as the boundary coordination processes of Communication Privacy Management theory (Petronio, 2002). Generally, it was expected that greater trust would facilitate the opening of communications boundaries in online social networks. Specifically, it was expected that:

> H4a: Trust in the OSN provider (TP) will positively influence OSN CPM
>
> H4b: Trust in all of one's OSN network connections (TAM) will positively influence OSN CPM, and
>
> H4c: Trust in one's close connections within their OSN network (TCC) will positively influence OSN CPM.

Although evaluation of the measurement model revealed issues with the measurement structure of the OSN CPM construct, results of the structural model were reviewed for cursory insight. These results suggested that each of the hypothesised paths was highly significant ($p < 0.001$) and that each type of trust influenced the inadequately defined OSN CPM construct. Specifically, TP had the strongest relationship with OSN CPM ($\beta = 0.307$) followed by TAM ($\beta = 0.198$)

suggesting that both trust in the provider and trust in all members were important in opening communication boundaries, but that organisational trust was more influential. Interestingly, trust in close connections (TCC) had a reasonably strong and significant negative impact on boundary coordination (β = -0.160, $p < 0.001$) suggesting that the more trust one had in close connections, the more they closed their communication boundaries. Although, it must be stressed that these relationships were observed through analysis with what was determined to be a flawed measurement instrument. Thus, even though there appeared to be support for H4a and H4b and a lack of support for H4c, these conclusions could not be drawn. Further, while reasons for the curious relationship observed between trust in close connections (TCC) and OSN CPM might be speculated, until an appropriate measurement model was incorporated, discussion was reserved.

7.2.2 Model Re-specification

As the discussion in Section 7.2.1 indicated, the hypothesised structural model required re-specification as a result of anticipated privacy concern and trust relationships not being realised and also because of the factor structure of OSN CPM being different than hypothesised. The re-specification was undertaken in a step-wise fashion with attention to the literature.

Organisational trust (Trust in the Provider, TP) was made an exogenous construct in the re-specified model. Given the lack of relationship between privacy concern and trust revealed in the hypothesised model results, it was thought these two constructs might function together in their influence on communication behaviour in OSNs rather than in dependent relationships. This was consistent with previously mentioned findings that identified trust as a moderating rather than mediating construct (Joinson et al, 2010) and treated trust and privacy concern as independent constructs (Dwyer, Hiltz and Passerini, 2007; Lin and Liu, 2012).

The re-specified final model also addressed the potential interconnectedness of interpersonal trust measures. Consistent with Luhmann's (1988) suggestion that building trust on the micro-level contributes to the determination of a more abstract form of trust on the macro-level, it was expected that the trust individuals have for those that are most closely connected (TCC) should determine the trust they have for the wider group of OSN members (TAM). Woolcock (1998) also rationalised a similar phenomenon with respect to social capital. Though in his writing about social capital, Woolcock (1998) conceptualised trust as a benefit of social capital rather than social capital itself, Putnam (2000) argued that trust was served as a good proxy for social capital, thus Woolcock's argument was still particularly relevant in this context. Specifically, Woolcock (1998) argued that social capital at the micro level was dependent upon one's intra-community ties, which he referred to as embeddedness, and also upon one's extra-community networks, which he referred to as autonomy. Thus, the trust among one's strong ties (TCC) should be related to one's trust in weaker ties (TAM), therefore this relationship was incorporated into the re-specified model.

Despite the interconnectedness predicted among strong and weak ties (TCC and TAM, respectively), a similar interconnectedness between TP and other trust constructs was not fully expected in the re-specified final model. Adler and Kwon (2002) carefully distinguished between social relations, hierarchical relations and market relations in relevance to social capital. Whereas trust in strong and weak ties (TCC, TAM) clearly pertained to social relationships, trust in the provider (TP) was conceptualised as a hierarchical relationship and thus these relationships should be distinct. However, given the argument above that trust in social relations might be generalised on the macro level from what is known on the micro level, it was also considered possible that the trust one held for the OSN provider with which they had experience might contribute to a generalised trust in all the members on the site (TAM).   Further, Adler and Kwon's (2002) own suggestion that there were likely characteristics of the various relations in all social structures, a relationship between TP and TAM seemed justified.

Privacy concern (CFIP) was also made an exogenous construct in the re-specified model. Trust was justified to be re-located as an exogenous construct, virtually no relationship existed between privacy concern and any of the three types of trust in the hypothesised model and the influence of privacy literacy measures (OK and SK) on CFIP was shown to be weak. Thus, there was no statistical evidence that supported the inclusion of privacy concern as an endogenous variable within this model. As the emphasis of this research was to determine the influences on OSN information sharing in light of privacy concern but not predict privacy concern, this was deemed an acceptable re-specification. Further, antecedents of privacy concern have been previously well established in the literature (Table 4.1). Finally, and most importantly, given strong evidence that privacy concern and trust do not function independently in information disclosures (Joinson et al, 2010; Lin and Liu, 2012) the possibility that CFIP worked in moderation with privacy literacy to effect OSN behaviours was thought to be an important investigation and thus incorporated in the re-specified model.

Additionally, model re-specification involved addressing the measurement model for the online social network communication privacy management (OSN CPM) construct which resulted in implications to the structural model. As analysis of the measurement model revealed that boundary ownership (BO) was not effective as measured and statistical evidence prevented its inclusion in the model, the BO construct was dropped. Analysis of the measurement model also revealed that boundary linkages (BL) and boundary permeability (BP), once trimmed of ineffective manifest variables, were sound measures of these constructs but OSN CPM could not be recognised as a second order construct representing the sub-dimensions of BL and BP. Thus, BL and BP had to be incorporated into the structural model raising questions about how the two constructs were related.

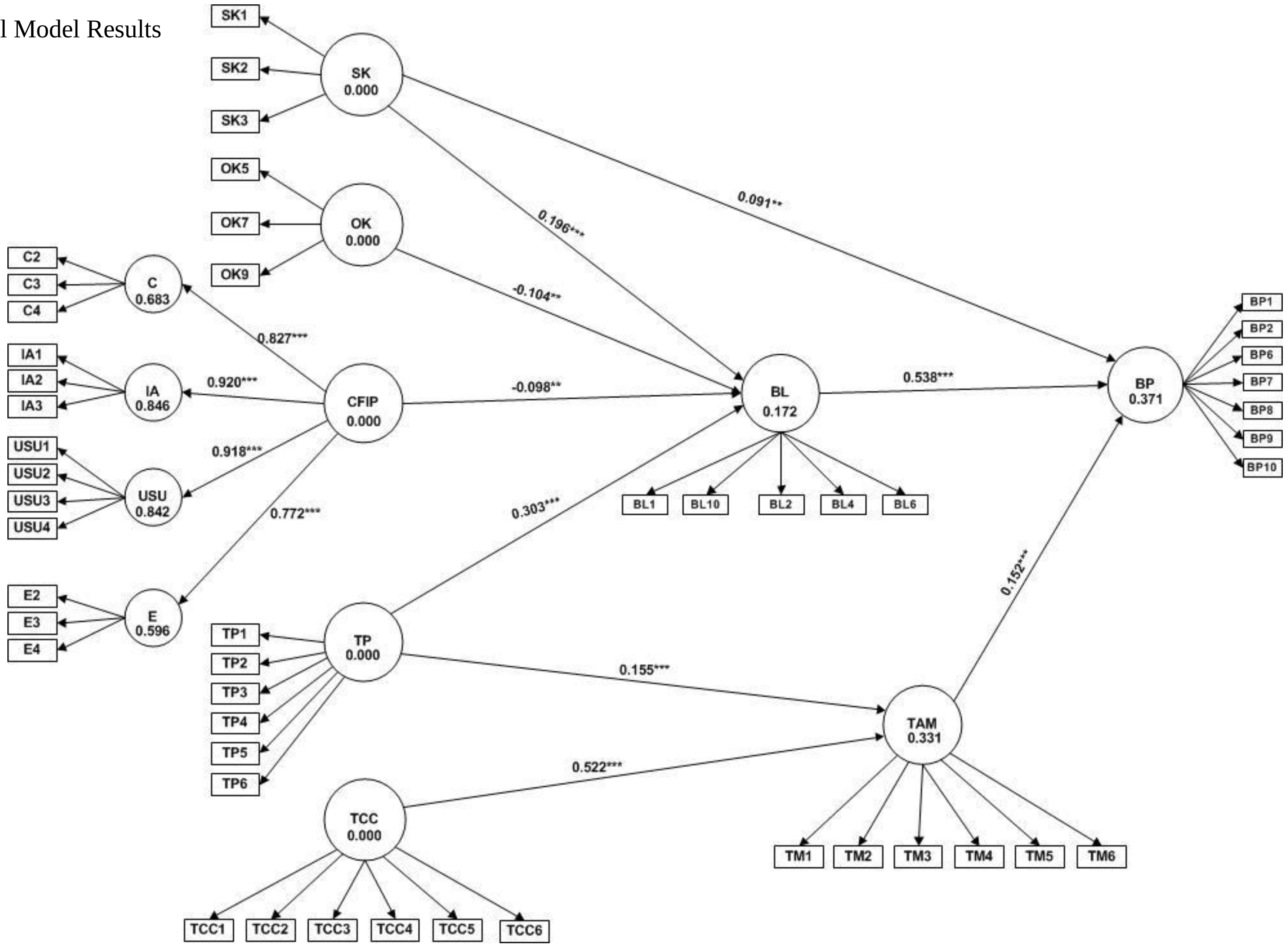
As CPM theory had only been tested empirically in one instance (Child, Pearson and Petronio, 2009), there was no confirmed theoretical basis upon which to restructure these paths. Instead, Petronio’s (2002) original publication of the theory was used to guide the practice. In her discussion of the boundary coordination processes of boundary ownership, boundary linkages and boundary permeability, Petronio (2002) clearly asserted that the processes need not be thought of as mutually exclusive. Indeed, she claimed that boundary linkages, permeability and ownership functioned in conjunction with one another to form the complete coordination process and that “boundary linkage has import for permeability” (p.88). Thus, the model was re-structured with a path connecting boundary linkages to boundary permeability.

As each of the newly exogenous constructs was originally hypothesised to influence OSN CPM, each was connected via structural paths to both BL and BP. And, as is appropriate in model development research (Hair, Ringle and Sarstedt, 2013), non-significant paths were removed as the analysis unfolded. Results of the final model achieved (Figure 6.2) have been discussed in Section 7.2.3. Figure 6.2 is also presented again in this section for reader convenience.

7.2.3 Final Structural Model Findings

Several interesting findings pertaining to the research objectives of this Project have been identified and discussed in this section. Among the most significant contributions of this research was the empirical confirmation that Communication Privacy Management boundary coordination processes were exhibited among OSN users. Further, results clearly showed that the connections established within OSNs (boundary linkages) and the breadth and depth of information shared among those linkages (boundary permeability) were indeed dependent upon privacy literacy, trust and privacy concern, at varying levels of importance. Observations about the effective influence of privacy literacy, trust and privacy concern on boundary coordination provided insight into the particular nature of those relationships. Thus, through interpretation of results of the final model, the second, third and fourth research objectives were accomplished. Specifically, the

Figure 6.2. Final Model Results



second research objective was to explain personal information disclosure in OSNs using CPM, objective three was to explain the role of privacy literacy in influencing OSN information disclosure decisions and objective four was to establish the role of trust in consumer OSN information disclosure behaviours. The first research objective – validation of a commonly used measure of privacy concern within a new context – had already been determined to be accomplished within the measurement model. However, there were interesting findings about the construct and its place within the final model that have as yet gone unmentioned. Therefore, the discussion that follows has addressed each of the major constructs within the final model including its contribution to understanding the privacy calculus and ability to accomplish the stated research objectives.

Privacy Concern

At the core of this Project was the goal of extending the privacy calculus literature by explaining the privacy paradox in ways that had previously been untested. Although some authors have reported an observed privacy paradox (Acquisti and Gross, 2006; Norberg, Horne and Horne, 2007) a comprehensive review of the empirical privacy calculus literature (Table 4.1) failed to isolate any studies that actually measured paradoxical privacy behaviour. Consistent with Rifon, LaRose and Lewis' (2007) assertion that a privacy paradox does not exist, each of the privacy concern outcomes measured in the literature identified behaviours that were consistent with actions that would be expected when privacy concern was present. For example, positive relationships between privacy concern and privacy protective behaviours, such as those revealed by Sheehan and Hoy (1999) and Wirtz, Lwin and Williams (2007), or negative relationships with information disclosure (i.e. Yang and Wang, 2009; Joinson et al, 2010; Lin and Liu, 2012) were not paradoxical at all. The major contributions from this Project, then, was the provision of empirical evidence of the privacy paradox and an explicative model using Communication Privacy Management.

Within the results, a privacy concern (CFIP) was clearly established. In fact, most respondents were highly concerned about their privacy as evidenced by the descriptive results (Table 6.3). The mean scores for the manifest CFIP items in the trimmed measurement model construct well exceeded the neutral point on the 7-point Likert scale; nine of the fifteen manifest variables had median scores of seven and four items had a median score of six. But, consistent with all other literature cited in Table 4.3, the direct outcome of CFIP noted in the model was not a paradoxical relationship. Indeed, CFIP negatively and significantly predicted boundary linkages (BL) in OSNs ($\beta = -0.098$, $p < 0.01$) meaning that higher privacy concerns would lead to fewer boundary connections. However, consistent with Dwyer, Hiltz, and Passerini (2007) who revealed little correlational relationship between privacy concern and information sharing on OSNs, the model also showed how the negative effect size of privacy concerns on boundary linkages was negligible ($f^2 = 0.011$). Thus, it appeared as though the significant relationship of privacy concern on boundary linkages was overcome by other contributing factors which positively influenced the breadth and depth of information sharing (boundary permeability). Consequently, the final model revealed information sharing in OSNs despite extremely high privacy concerns, also known as the privacy paradox, and offered an explanatory mechanism of the phenomenon.

This finding was particularly intriguing as it raised questions about the need to measure privacy concern at all. The literature review identified a great deal of contention over how privacy should be defined and ultimately conceptualised (Sections 3.1.2 and 3.1.3) and though privacy was argued to be valuable herein, there were claims that privacy had died in this new technological era of ubiquitous information sharing and arguable oversharing (i.e., Meeks, 2000). The findings produced in this study provided answers to these two contentious issues. First, results clearly established that privacy concern was alive and thriving and second, privacy concern could be effectively measured using CFIP. In fact, results indicated that respondents held high concern about each dimension of privacy concern. Namely, respondents were concerned about what information was collected about them, concerned about instances where their personal information might be improperly accessed or used in unauthorised ways and also concerned about errors that might exist with their personal information that has been collected. But, results also demonstrated that those high levels of privacy concern did very little to decrease the connections established within OSNs. Instead, other factors including confidence and trust compensated for privacy concern to permit connections and information sharing in online social networks.

Therefore, results suggested that perhaps privacy concern should be assumed. Where privacy concern levels were so high and they did little to reduce information sharing, it appeared that practical implications of this research should emphasise concentration upon the other factors that influence information disclosure (such as those identified in Table 4.1, p.139). Inclusion of a privacy concern measure in future research will still be warranted, however. Further research into the privacy calculus or that offering longitudinal or cross-cultural comparisons will still require measurement of the construct. In those instances, use of CFIP would be recommended as a result of this study.

OSN Communication Privacy Management

The results also offered important insight into how Communication Privacy Management can both be measured and how it operates within OSNs, thus accomplishing the second research objective of this Project. Though CPM had been used as a theoretical guiding framework in previous research (Metzger, 2007; Xu et al, 2011), the criteria for boundary rules were shown to be exhibited in Facebook (Waters and Akerman, 2011), and the three dimensions of CPM were confirmed among online bloggers (Child, Pearson and Petronio, 2009), the theory had not been quantitatively tested in OSNs. As discussed previously, valid and internally reliable measures of the boundary linkage and boundary permeability dimensions of OSN CPM were established from this analysis. However, as the construct was shown to also be first-order, how these two dimensions interacted with each other was an important additional conclusion derived from this research. Indeed, the dependence association between the BL and BP constructs were revealed to be the most significant relationship in the final model ($\beta = 0.538$) meaning that decisions about connections made in OSNs was the most important predictor of the breadth and depth of information shared in those environments.

Such a finding made intuitive sense and had been suggested by Petronio (2002) in the theoretical presentation of CPM theory. Further, Cespedes and Smith (1993) did suggest that the information collector could influence one's privacy threshold. In addition, it may also have been inferred from other empirical research concluding that the sensitivity of information requests influenced information disclosure (i.e., Yang and Wang, 2009) that the receiver of the information predicted whether information was disclosed. However, this finding was thought to offer a significant contribution with relevance to the academic understanding of privacy. As OSN connections are comprised of various types of connections including close and weak ties, thus this finding suggested that decisions about information disclosure are being made as a result of the unique relationships within that collective. And as the empirical evidence in the literature that suggested information sensitivity determined disclosure did not specifically measure the role of the recipient in the information exchange. Therefore, this finding was considered a unique contribution that served to objectively support Petronio's (2002) conceptually derived suggestion that boundary linkages were important for boundary permeability.

Not only was the relationship between boundary linkages and boundary permeability the most significant revealed in the model, it was also determined that connections (BL) had the largest effect on information sharing (BP) among all predictive constructs. However, confidence in privacy knowledge ($\beta = 0.091$, $p < 0.01$) and trust in weak ties within the OSN network ($\beta = 0.152$, $p < 0.001$) were also shown to directly influence the breadth and depth of information shared. Findings revealed that the more confidence one had in their privacy literacy (SK), the more information they shared (BP) and the more open they were with the connections established in OSNs (BL). Similarly, the higher the trust one had for their weak connections in their OSN networks (TAM), the more information they shared.

These findings were particularly interesting when considered with results previously discussed pertaining to privacy concern. Indeed, it would appear that despite holding privacy concerns about OSNs, if one felt confident in what they knew about privacy, they were more likely to share greater amounts of information, but that confidence was more important in dictating OSN connections than in directly influencing information disclosure. Similarly, it appeared from results that trust was a powerful predictor of information disclosure that was able to overcome the restrictions that privacy concern might ordinarily exert upon information exchange. For, in addition to the direct influences observed in the final model, how much one trusted their OSN provider (TP) and how much one trusted their strong ties (TCC) also indirectly influenced the extent of information sharing within OSNs. However, the influence of trust was observed to be more effective in explaining the mediating constructs of linkages and trust in weak ties as opposed to information disclosure (Table 6.19). Finally, privacy knowledge accuracy and privacy concern negatively influenced information disclosure, but the effect was negligible. Instead, privacy knowledge and privacy concern were exhibited in communication privacy management as restrictions upon boundary linkages that were less effective than the positive influences of confidence and trust.

As a result, the exogenous constructs explained communication privacy management via effects observed upon the mediating constructs of boundary linkages and trust in all members. Accordingly, a number of important insights were determined with respect to the influence of exogenous constructs upon the connections made with OSNs (BL). Privacy concern (CFIP), as already explained, reduced the connections made in OSNs. Privacy literacy (SK and OK) and trust in the provider (TP) also exhibited significant dependent relationships with boundary linkages. As the third objective of the research was to explain the role of privacy literacy in influencing OSN information disclosure decisions and objective four was to establish the role of trust in consumer OSN information disclosure behaviours, these findings were particularly important. However, as each of these insights pertained to other research objectives, they have been discussed in subsequent appropriate sections.

Privacy Literacy

Privacy literacy had both direct and indirect effects on communication privacy management. Specifically, Subjective Knowledge (SK) had significant direct effects on boundary linkages ($\beta = 0.196$, $p < 0.001$) and significant direct ($\beta = 0.091$, $p < 0.05$) and indirect effects ($\beta = 0.196$) on boundary permeability. Although the significant effects of subjective knowledge on boundary permeability were negligible in the context of the entire model, the effects of subjective knowledge on boundary linkages that was found to be the most important contribution of subjective knowledge within the final model. And, although objective knowledge had a negative and significant effect upon boundary linkages ($\beta = -0.104$, $p < 0.05$), it did not account for as much of the effect on boundary linkages as subjective knowledge.

From the results, it appeared that the confidence one had in their privacy knowledge was directly related to the connections made in OSNs. And, that confidence exhibited a much stronger effect ($f^2 = 0.045$) on OSN connections than the other privacy literacy measure - one's objectively determined privacy knowledge (OK $f^2 = 0.012$). Thus, the decision making control afforded by privacy literacy was driven by one's subjective assessment, or perceived knowledge, rather than actual knowledge. These results suggested that individuals confident in their privacy knowledge might also have been under the impression that they knew enough to protect themselves from privacy risks and thus were afforded the confidence to form linkages in OSNs.

However, thinking you know something is not the same as knowing it. So while these results demonstrated that confidence in privacy knowledge was more important in predicting connections made in OSNs, the results did not suggest what might happen to the complex relationship if objective knowledge was higher among the sample or if the construct had been measured differently. Since the results established that objective knowledge significantly reduced boundary linkages, a dependence relationship could be concluded. However questions remained about the quantitative assessment of this measure as discussed in Section 7.1. Specifically, descriptive results indicated that objective privacy knowledge was generally low among respondents (Table 6.1) and the only manifest objective knowledge items determined to be psychometrically appropriate were those to which most respondents knew the answer. In addition, the objective knowledge scale resulting from measurement model trimming was determined to represent only items that represented very general common knowledge rather than a breadth or depth of understanding about privacy.

Furthermore, in light of results of this study, there were concerns that low levels of accurate privacy knowledge could be increasing an individual's privacy vulnerability. As was clearly revealed through this research, the more one knew about privacy, the more restrictive they were with linkages established in OSNs and those connections ultimately influenced the extent of information sharing. However, in the face of low objective knowledge, other factors including confidence and trust were more important in opening privacy boundaries and allowing information exchange. Since few people knew a lot about privacy (Table 6.1), and privacy risks are not necessarily derived from individual pieces of data exchanged (Acquisti and Gross, 2009), the argument could be made that people need to know more about privacy in order to make sound decisions about information disclosure in OSN environments.

Particularly, Acquisti and Gross (2009) recently revealed that an individual's date and state of birth were sufficient to guess his or her Social Security number with great accuracy thereby illustrating the power available within personal information that might appear innocuous. Similarly, Kosinski, Stillwell, and Graepel (2013) just revealed that numerous personal characteristics could be identified simply through one's Facebook 'likes'. Specifically, patterns of likes could be modelled to successfully predict gender, ethnicity, age, religious and political orientations, sexual orientation, parental marital status and use of addictive substances. Further, it was also recently revealed that the United States National Security Agency (NSA) had direct access to consumer data shared with Internet companies including Google, Facebook and Apple and that the NSA shared that information with other countries' security agencies (Greenwald and MacAskill, 2013). As global public outrage over the NSA surveillance scandal has taught, society as a collective has not been aware of all of the information being collected about individuals, nor has it been aware of the ‘silent listeners’ (Stutzman et al, 2012) that can access their personal information, or how that information may be combined, or the implications of those combinations to their personal privacy. Indeed, as Naughton (2013) convincingly asserted about the incident, “Most people would be discomfited to learn how detailed a reconstruction of their lives their mobile phone operator could produce if required – right down to a pretty good guess at when they have been speeding in their cars.” But, this poor awareness is not a new observation, either. The incident with the NSA has reinforced claims that have been made over the last decade that individuals do not know enough about privacy or the implications of how their information is used (Cavoukian and Hamilton, 2002; Solove, 2006; Nissenbaum, 2010).

Therefore, since accurate basic knowledge about privacy was shown to restrict privacy boundaries, a logical extension of the argument becomes that greater privacy knowledge might restrict those boundaries further, perhaps even to a threshold where that knowledge would become more important than either confidence or trust within the privacy calculus. Thus, there is an opportunity for future research to investigate the differences that might exist when tests of the model are conducted on individuals with high objective knowledge and low objective knowledge separately. At a minimum, however, the evidence herein suggested that privacy knowledge did offer decision making control about information disclosure behaviour and therefore increased privacy knowledge would afford individuals increased control over their privacy decisions. Thus, findings about objective knowledge had implications for government and business and academic study as will be discussed in Chapter 8.

Trust relationships

The results contributed interesting insights with respect to the effects of different types of trust on each other and on each of the dimensions of communication privacy management in OSNs. In total, three different kinds of trust relationships were examined - organisational trust (TP), and interpersonal trust including that among strong ties (TCC) and weak ties (TAM).

Organisational trust was found to contribute to both boundary linkages and boundary permeability. Specifically, trust in the provider (TP) was found to directly and significantly influence boundary linkage ($\beta = 0.303$, $p < 0.001$), directly and significantly influence trust in all OSN members ($\beta = 0.155$, $p < 0.001$) and indirectly influence boundary permeability (total effects = 0.187) through its relationship with trust in all members (indirect effects = 0.024) and boundary linkages (indirect effects = 0.163). Examination of the effect size of these relationships revealed that organisational trust was particularly important in determining connections established in OSNs ($f^2 = 0.109$) and weakly contributed to the variance extracted in the measure of trust in all members ($f^2 = 0.034$), but as mentioned previously, negligible in determining boundary permeability ($f^2 = -0.002$).

These results showed that trust in the provider was essential in predicting the breadth and depth of information shared in OSNs, but only indirectly. This observation can be loosely compared to Metzger's (2007) finding that privacy assurance influenced personal information disclosure to an online company. As privacy policies have been shown to represent symbols of trust (Pan and Zinkhan, 2006), there was the expectation that organisational trust would influence information disclosure in OSNs, a relationship that was notably observed in the results.

However, what made this study's findings about organisational trust particularly interesting was the way in which trust in the provider influenced information disclosures – through boundary linkages. Among all the influences on boundary linkages observed in this Project, trust in the provider had the strongest effect size ($f^2 = 0.109$). This means that while both subjective knowledge ($f^2 = 0.045$) and trust in the provider were shown to be able to counteract the negative influences of objective privacy knowledge and privacy concern on boundary linkage, trust in the provider had the most dramatic influence.

This result was particularly interesting when considered alongside conclusions drawn from relationship management literature. Particularly, in contrast to results that showed organisational trust influenced information disclosure intentions in the context of direct marketing (Schoenbachler and Gordon, 2002), the findings of this study indicated that the effect of organisational trust in the model was upon the connections established in OSNs rather than on disclosure behaviours directly. However, consistent with Milne and Boza's (1999) finding that organisational trust was a more effective marketing strategy than attempts to reduce privacy concern, results of this study indicated that organisational trust was a much stronger influence upon OSN behaviours than privacy concern. Inferred from this result were important managerial implications.

Particularly, since trust in the provider was the most important contributor to boundary linkages, review of the manifest items of the boundary linkage measure provided additional insight to this relationship. The final boundary linkage scale (Table 7.1) included items measuring connections to other OSN participants (BL1, BL2 and BL4) but also to other organisations including external websites (BL6) and application providers (BL10). The suggestion in these findings was that one uses their trust in the provider to justify links with all connections facilitated by the OSN – both interpersonal and organisational.

Where most OSNs are free services, the provider companies generate revenue primarily from advertising revenue[10] (MSN Money Partner, 2012) and the connections that member participants make within the provider's network then become critical to the success of its business model. First, OSN providers require a critical mass of participants to substantiate an argument to advertisers that their service has sufficient reach and warrant the advertising fees charged. Second, since user motivation to participate in OSNs is predicated upon perceptions of social capital (i.e. Lampe, Ellison and Steinfield, 2006), and social capital is only a potentiality when there is access to social connections (Coleman 1988; Nahapiet and Goshal 1998; Valenzuela, Park and Kim 2009), achieving a critical mass of users to generate advertising revenue becomes dependent on members establishing interpersonal connections within the OSN platform. Third, virtual communities such as OSNs have been recognised to offer brands an important platform within which to enact social customer relationship management strategies (Faase, Helms and Spruit,

[10] Approximately 82% of Facebook's revenues are generated through the sale of advertising space. The remainder of revenues are derived from commissions on virtual goods users purchase from game applications (MSN Money Partner, 2012)

2011). If the OSN provider offers a platform upon which participants willingly connect with advertisers and their associated content, advertisers will view the platform as a useful outlet for their advertising expenditures. Therefore, both the interpersonal and organisational linkages established on their platforms are critical to the financial viability of the OSN provider.

Since results suggested that trust in the OSN provider was the most important influence upon the linkages established within OSNs and linkages have been argued to be critical to the financial success of the OSN, it follows that OSN providers' financial health would be dependent upon the amount of trust member participants had for the OSN provider. Therefore, OSN providers must carefully consider how trust is established with their members and avoid violating that trust since Petronio (2002) argued that boundary turbulence, or violations in privacy rules, would ultimately upset communication privacy management and Morgan and Hunt (1994) similarly argued that any abuse of information would result in a loss of trust for the organisation. It is reasonable, then, that OSN providers take precautions to preserve the trust they have currently and seek ways to advance greater trust whether by organisational reputational development (Eastlick et al, 2006) or otherwise (Schoenbachler and Gordon, 2002).

Indeed, balancing issues of organisational trust will be particularly critical for online social network providers as they try to strike a balance between revenue generation and the privacy interests of their members. For instance, in 2007 Facebook faced public outcry about privacy violation when it launched Beacon – a partnership with corporate advertisers that resulted in purchases made with partner online retailers being announced on the purchaser's Facebook Newsfeed. Sensing the boundary turbulence created by Beacon, Facebook eventually removed the feature. And, when Burger King ran a promotion via a Facebook app in 2009, Facebook again forced some functionality of the app be disabled due to privacy concerns. Burger King's promotion, entitled the 'Whopper Sacrifice', involved Facebook users publicly unfriending Facebook connections in exchange for a free whopper. This induced boundary turbulence because within the Facebook platform unfriending connections ordinarily did not entail notification. Since this public posting was comparable to the trust-jeopardising boundary turbulence associated with Beacon, Facebook likely engendered a reputational boost from some users when it disabled the app, although it also demonstrated the tricky spot Facebook could find itself in with respect to balancing the interests of advertisers with those of its members.

Interpersonal trust relationships also yielded interesting insights from the final model. The relationship between trust in close connections (TCC) and trust in all members (TAM) was the second strongest dependence relationship revealed in the final model ($\beta = 0.522$, $p < 0.001$) and demonstrated a strong effect ($f^2 = 0.389$). Although the privacy literature did not distinguish between these types of trust, the relationship was consistent with theoretical conceptual assertions of social capital at the micro level influencing social capital at the macro level (i.e. Luhmann, 1988; Woolcock, 1998). Thus, this relationship supported the notion that we may generalise our trust in a wider group based upon the trust we have in our close connections. Considering OSN networks are comprised of those we know well (close connections) and those we know less well (weak ties) and our information may also be viewed by an even larger group of individuals of people we do not know including friends-of-friends or, depending upon privacy settings applied, even the public at large, empirical support for the extension of trust in distant connections was an interesting revelation.

However, interpersonal trust was not found to influence the connections made within OSNs. Although Petronio (2002) surmised that boundary links "may vary based upon the strength or weakness of the ties that bind the privacy boundaries and the people in them" (p.91), neither trust in close connection nor trust in all OSN members had a significant influence on boundary linkages. Instead, it was the trust in the provider that most significantly influenced boundary linkages ($\beta = 0.303$, $p < 0.001$).

Further, social capital has been argued to be influential in information exchange (Nahapiet and Ghoshal, 1998) and trust had been argued to be a dimension of social capital (Paldam, 2000; Putnam, 2000; Scheufele and Shah, 2000), or a good proxy for it (Putnam, 2001). Thus, the finding herein that trust in all members (akin to bridging social capital) had a direct and significant influence upon information sharing in OSNs ($\beta = 0.152$, $p < 0.001$) was consistent with expectations. Similarly, the indirect effect of trust in close connections on breadth and depth of information sharing (indirect effect = 0.281) suggested that bonding social capital was also influential in the process. Despite the strong dependence relationship noted, however, the effect size of trust in close connections upon boundary permeability was negligible ($f^2 – 0.000$). Therefore, while trust in close connections was determined to be a strong predictor of more generalised trust in all members, it was the generalised trust in all members that better explained boundary permeability in OSNs.

7.3 Concluding Remarks

Communication Privacy Management theory provided a unique and effective way to understand information disclosures in online social networks when privacy concerns were evident. Privacy concern was shown to reduce the boundary connections made in OSNs, but not by so much as to restrict information disclosure in those environments. Thus, a privacy paradox was realised in this analysis. The results also offered an explanation of that privacy paradox via a privacy calculus that included privacy literacy and trust. Specifically, confidence in privacy knowledge and trust in the provider had enough of a positive influence on boundary linkages to overcome the negative effects of privacy concern and objective knowledge to permit OSN connections. And, interpersonal trust showed a sufficiently strong and positive influence the breadth and depth of information shared on OSNs.

Interestingly, while the more one accurately knew about privacy restricted the boundary linkages established in the environment, that knowledge had an insufficiently strong influence on the information disclosure decisions taken by respondents. Instead, how much one thought they knew about privacy was a significantly more powerful privacy literacy influence in the information disclosure decisions taken. Those particular results also raised questions about what influence expanded privacy knowledge might have upon the process. As the sample of respondents possessed low levels of objective knowledge and the objective knowledge scale retained in the measurement model only included items reflecting the most common knowledge about privacy, it was questioned whether more objective knowledge might serve a greater restrictive capacity on the connections made in OSNs.

Both organisational and interpersonal trust were also shown to affect communication privacy management but in different ways. Whereas organisational trust was most significantly associated with boundary linkages, interpersonal trust did not affect the connections made within OSNs. Instead, interpersonal trust was determined to affect the breadth and depth of information shared in OSNs. The interdependence of the various kinds of trust was also established.

But, the results of this analysis also suggest that perhaps privacy concern should be assumed to be held by most. Contrary to assertions that privacy no longer exists (Meeks, 2000; *in* Johnson, 2010; Lipschultz 2012) in digital communication environments, concern over personal information privacy has been well established. Public opinion reports have suggested privacy concern is becoming more prevalent in the population (Westin, 2003) or at least holding steady with only a minority unconcerned (Direct Marketing Association, 2012) and the descriptive results captured in this study reflected very high levels of privacy concern (Table 6.3). When combined with conclusions that privacy concern was not the most influential factor in predicting OSN behaviours both herein and in other studies (Joinson et al, 2010; Lin and Liu, 2012), these observations suggest that the measurement of privacy concern is less important. Instead, identifying the influences that allow an individual to overcome high levels of privacy concern is, arguably, of greater importance.

8 Conclusions

At the time of this research, online social network participation was approaching ubiquity in the Western world. In the context of OSNs, where information disclosure is requisite to achieve social capital benefit, privacy concerns have also been acknowledged among participants. Thus, this research sought to investigate the ways in which this privacy paradox might be explained. Although investigations of the privacy calculus used by individuals to overcome privacy concerns had been conducted, there were gaps in the literature suggesting that additional factors in the calculus might further explain the paradoxical phenomenon. Moreover, despite conceptual support for Communication Privacy Management (CPM) theory to explain information exchanges, the information boundary coordination processes had not previously been empirically tested in OSNs. Furthermore, comparison of results from previous studies was challenged due to inconsistent operationalization of a privacy concern measure. Therefore, this Project maintained four primary objectives: i) to validate a prominent conceptualization of privacy concern in the context of online social networks, ii) to explain personal information disclosure in online social networks using Communication Privacy Management theory, iii) to explain the role of privacy literacy in influencing online social network information disclosure decisions, and iv) to establish the role of trust in consumer information disclosure behaviours in online social networks.

As a result of the insights derived from each of the Project's specific research objectives, a number of important contributions were identified. The research contributions will be discussed in Section 8.1. The limitations associated with this

Project are discussed in Section 8.2 and the various implications of the study conclusions are presented in Section 8.3.

8.1 Study Contributions

As revealed throughout the discussion, there were several contributions of this research. Contributions of this study have been presented according to the four main research objectives established for this Project in Sections 8.1.1 through 8.1.5.

8.1.1 Contribution from Objective 1

The first stated objective of this research was to validate a prominent conceptualization of privacy concern in the context of online social networks which was accomplished via results supporting the acceptance of CFIP as a valid and internally reliable measure. As a measurement, CFIP was validated in the context of OSNs with Canadian respondents, thereby offering additional support to the external reliability of the measure. Further, despite claims of the contextual nature of privacy concern throughout the literature, validation of CFIP in yet another context and culture suggested that CFIP was a strong measure with more universal application than originally thought by its authors (Smith, Milberg and Burke, 1996). This was an important contribution of the research. The additional support found for this measurement instrument suggested that CFIP may be a sufficient measure to be used in future privacy concern investigations, thus permitting cross comparison of privacy concern research conclusions rather than continuous propogation of the disparate collection of findings available today.

To be clear, results of this study did not conclude that CFIP was the best measure of privacy concern as tests of other instruments were not employed. Indeed, support for other privacy concern measures were found in the literature including Malhotra, Kim and Agarwal's (2004) Internet User Information Privacy Concern measure (Buchanan et al, 2007; Yang and Wang, 2009). However, the validation of CFIP offered by this study did permit the conclusion that the measure was psychometrically sound and applicable to the environmental context of OSNs and within the regulatory and cultural context of Canada.

8.1.2 Contribution from Objective 2

Results suggesting that information disclosure in online social networks could be explained using Communication Privacy Management (CPM) theory was an important contribution of this study as it represented the first empirical support of its kind. In addition, the results of the study also provided insight to both how the OSN CPM construct was measured and how it operated in this context and thus represented valuable related contributions.

In terms of measurement of OSN CPM, results of this study revealed effective measurement models for two dimensions of OSN CPM – boundary linkages (BL) and boundary permeability (BP) – but, not for the third dimension (BO). Findings from the OSN CPM measurement model analysis did not support the inclusion of all items derived from Child, Pearson and Petronio's (2009) Blogging Privacy Management Measure (BPMM) nor the second-order factor structure of the construct offered by the authors. Structurally, OSN CPM was influenced differently by privacy literacy, privacy concern and various types of trust. Accordingly, this research contributed the following understandings about OSN CPM: i) personal information boundary coordination via BL and BP in OSN contexts was evident, ii) parsimonious measurement models of BL and BP constructs were offered, iii) though distinct, BL and BP were dependent, and iv) future research should aim to confirm these findings and continue to explore appropriate measurement instruments for boundary ownership (BO).

8.1.3 Contribution from Objective 3

To investigate the third research objective of explaining the role of privacy literacy in online social network information disclosure decisions, privacy literacy was hypothesised to be negatively associated with privacy concern. Specifically, privacy literacy was conceptualised as two distinct constructs - objective and subjective knowledge - that operated independently to influence privacy concern. Whereas the measurement model for subjective knowledge originated in the literature, no privacy objective knowledge scale existed and thus had to be created. Significant dependence relationships between both subjective knowledge and privacy and objective knowledge and privacy concern were observed. However, in contrast to the hypothesised relationship, the dependence among objective knowledge and privacy concern was found to be negative and the relationships between privacy literacy and privacy concern were found to be insufficient to explain much of the variance in privacy concern. Instead, rather than exhibiting a mediated influence on the OSN boundary coordination processes of boundary linkage and boundary permeability through privacy concern, results supported the notion that the influence of privacy literacy was direct.

Accordingly, this research contributed the following understandings about privacy literacy in OSN information disclosures. First, objective knowledge and subjective knowledge functioned in opposing ways. Objective knowledge reduced boundary linkages whereas subjective knowledge was positively associated with OSN connections (boundary linkages). Second, one's confidence in privacy knowledge (subjective knowledge) was more influential than privacy knowledge accuracy (objective knowledge) in predicting boundary linkages. Third, subjective knowledge also directly influenced the extent to which information was shared in OSNs (boundary permeability), but its weak effect also suggested that subjective knowledge contributed the most to the privacy calculus investigated via its influence on boundary linkages. Fourth, questions were raised about the objective knowledge measurement model. While determined to be valid and internally reliable, future research should aim to explore alternative measurement instruments.

8.1.4 Contribution from Objective 4

The remaining research objective sought to establish the role of trust in consumer information disclosure behaviours in online social networks. Whereas privacy calculus literature had emphasised the relationship among organisational trust and privacy concern, no study had empirically tested the dependence relationship between interpersonal trust and privacy concern. Thus the inclusion of both types of trust in the hypothesised model of this Project provided a novel conceptualisation.

Results associated with the role of trust in OSN information disclosures provided some interesting conclusions as well. First, as mentioned previously, dependence relationships between privacy concern and any type of trust were not found. This was particularly revealing as the literature suggested contradictory findings with respect to organisational trust and privacy concern findings. This conclusion further supported arguments that privacy concern and trust function independently in the privacy calculus. Second, trust in the provider was found to exert a strong effect upon OSN connections (boundary linkages), more so than any other construct in the model. Thus, trust in the provider was thought to be critical in overcoming privacy concerns to facilitate information disclosure in OSNs. Third, concurrent with social capital literature suggesting generalisation from micro to macro contexts, trust in all members of an OSN network was found to be dependent upon trust in close connections. Fourth, though strong relationships between trust in close connections and trust in all members were concluded, interpersonal trust exhibited little effect on information disclosures in OSNs.

8.1.5 Further Contributions

In addition to the direct contributions derived from each of the four research hypotheses, there were other contributions observed from this investigation. Most importantly, integration of each of the research objectives resulted in the successful validation of an explanatory model of the privacy calculus using a novel conceptualisation of information disclosures – Communication Privacy Management – and incorporating previously untested relationships. Further, whereas other privacy calculus research failed to empirically demonstrate information behaviours paradoxical to privacy concern, the model offered in this research established both the existence of the paradox along with an explanatory mechanism. However, results showed very high privacy concerns that exerted minimal influence on OSN behaviours. Thus, results also suggested that privacy concern should be assumed and that attention be paid to the factors that have been revealed to be capable of overcoming those concerns – subjective knowledge and trust in the provider. Alternatively, attention to a factor shown to inhibit connections within OSNs – objective knowledge – was also suggested to have merit in future research and practice. Particularly, as incidents of boundary turbulence such as privacy breaches are made public, OSN participants may associate greater importance with objective knowledge and increase their privacy literacy. This potentiality and hypothesised effects would be an interesting avenue for future research.

In addition, this research provided another contribution by way of the Canadian perspective. Results were reasonably consistent with assertions within literature developed in other contexts, which could suggest that the Canadian context did not offer any particularly unique insights. However, it is maintained that confirmation of observations in a Canadian context did offer value The results of this study provided external validation of pre-existing constructs and relationships while also contributing an understanding of attitudes and behaviours from a population under-represented in privacy studies.

8.2 Study Limitations

There were several limitations to this study that required caution in interpretation of findings and presented opportunities for future research. One important limitation was the narrow focus of the research model. The literature identified a number of other influences within the privacy calculus and several antecedents to privacy concern had been isolated (i.e., Xu et al, 2011), yet the model herein did not test all possible relationships. Instead, the relationships tested in this model were selected due to their potential to reveal new insights into the privacy calculus. As the survey instrument consisted of 82 manifest variables and 13 descriptor items and took respondents in excess of fifteen minutes to complete, participation rate and/or completion rate might have been adversely affected by the inclusion of other items in this study. Nevertheless, future research should consider ways to incorporate additional previously tested relationships to provide a more complete understanding of the privacy calculus in light of these new findings. The parsimonious Communication Privacy Management scale derived from this Project could be used to that end.

The generalizability of results was also limited due to the snowball technique of data collection. The snowball sampling technique did provide access to a broader group of respondents than research commonly based upon convenience samples of university students. And, the sample achieved was ultimately considered to be generally representative of the OSN user. However, the snowball sampling technique did also have serious limitations. First, similarity bias is a possible risk when snowball techniques are employed. As the snowball in this research began with survey invitations extended to the researcher’s own contacts within OSNs, the risk of similarity bias with the researcher was a real concern. While some of these risks were thought to be minimized by the very nature of OSN friend network composition which includes both strong and weak ties that permit diversity of information, the possibility that respondents held attitudes and OSN behaviours too similar to the researcher and each other to be generalizable was an issue that cannot be ignored. Second, generalizability of results outside of Canada was not possible as assessment of objective knowledge was done through the very concentrated lens of *PIPEDA*, the omnibus privacy legislation specific to Canada. Although, future research might seek to establish similar relationships within countries that maintain similar universal privacy laws, there was no expectation that these results would generalise to other regulatory environments. Third, generalizability to non-Western cultural contexts would be challenged. Another potential criticism of this research was that it represented yet another sample drawn from a Western, Educated, Industrialized, Rich, and Democratic (WEIRD) society (Henrich, Heine and Norenzayan, 2010).

Methodological limitations pertaining to research design were also identified with this research. The research design justified an embedded mixed method that used focus groups to enrich the survey instrument but emphasised a quantitative, positivist perspective. Where positivist approaches accentuate standardisation and objectivity, inclusion of a ‘less rigorous’ (Shah and Corley, 2006) focus group method could raise philosophical objections, although the embedded design minimized these concerns (Creswell and Plano Clark, 2011). Moreover, as the quality of focus group research is heavily dependent upon moderator skill (Stewart and Shamdasani, 1990), it stands to reason that experience would be important in developing said skill. As the focus groups conducted in this Project represented the first ever conducted by the researcher, moderator skill was determined to be an additional limitation of this Project.

Further, caution need be exercised in interpreting results of this study. Although SEM depicts relationships as causal and results are typically discussed in the manner of one construct 'influencing' or 'having an effect' on another, as was clearly established in Section 7.2, the results of this study demonstrate dependence relationships but do not confirm causality.   And finally, the skewed and kurtotic statistical properties of privacy concern (CFIP) suggested in Section 6.1.3 required further caution in interpretation of results. Although PLS analysis does not require normally distributed responses, highly kurtotic and/or skewed responses may create interpretive difficulty (Hair et al, 2013). While the results indicated that privacy concern functioned as it should have based on the literature and intuition, the non-normal statistical properties of the measure were a possible limitation on the results.

8.3 Implications

A new model for understanding information disclosure decisions in online social networks was conceptualized and successfully estimated (Figure 6.2) among a sample of Canadian online social network users. The results have implications for the science of marketing, for management and also for government.

Implications for the science of marketing

Results reinforced constructs and relationships reported in the literature, provided empirical support for new constructs and hypothesised relationships and signalled areas where future research opportunities exist. Thus, there were numerous implications to the science of marketing.

Support for previously established constructs was revealed in the results. While PLS-SEM was not a statistical confirmatory technique, the external validation of these constructs in the context of this study provided additional evidence to support the stability of the following measures:

- The CFIP construct, commonly used to assess personal information privacy concerns in the literature, was validated again through this research. Measurement consistency is essential to compare findings among studies. In fact, one of the common challenges with interpreting the vast privacy literature has been the lack of definitional consistency. Thus, future research should utilise constructs that have consistently been validated. Based upon the results of this research, CFIP represents one such construct.
- Although modified from its original context and trimmed due to focus group input, the SK construct contributed by Carlson et al (2007) was found to be a psychometrically sound, parsimonious (3 item) measure of consumer confidence in privacy knowledge.
- Organisational trust (TP) and interpersonal trust (TAM) previously validated by Krasnova et al (2010) received further validation in this study, suggesting the measures were psychometrically sound.

Similarly, one structural relationship supported similar claims identified in the literature. However, rather than supporting the existence of the relationship, this study supported claims that a dependence relationship between CFIP and Trust did *not* exist.

A number of novel relationships were identified in the structural model. The following observations represent the specific unique contributions of this research and thus require external validation in future studies.

Communication Privacy Management boundary coordination processes were empirically defined in a singular study situated in the context of blogging, but application in the context of online social networks had not previously been assessed. This research yielded unique findings about both the measurement model for OSN CPM and the structural paths among its dimensions. Specifically, only the dimensions of BL and BP were supported in this OSN context and each was ultimately determined to be measured differently than in the original operationalization by Child, Pearson and Petronio (2009). Future research should attempt confirmation of the parsimonious measures offered for each BL and BP. And, because this analysis failed to produce a reliable measure of BO, future research should look at other ways in which boundary ownership can be operationalized both in the context of OSNs and in alternate situations.

A measurement model for OK was tested for the first time in the context of OSNs and was determined to be valid, reliable and somewhat influential in OSN CPM. However, the measure used herein was developed specifically to represent the Canadian regulatory context; future research should investigate alternate measures of objective knowledge that can be generalizable to other contexts.

A number of structural paths had been identified for the first time in this research as well. Specifically, this remains the only validation for the following paths:

- BL → BP
- SK → BP
- SK → BL
- OK → BL
- CFIP → BL
- TP → BL
- TP → TAM
- TCC → TAM
- TAM →BP

Thus, additional tests in different contexts are required to establish general validity of the model. In particular, the results generally suggest that future studies use OSN CPM to understand the unique and complex information disclosure processes in OSNs. The significant effect revealed for subjective knowledge on BL suggests that future studies of privacy calculus should incorporate subjective knowledge to provide a more comprehensive explanation of the privacy paradox. In addition, the significant, but overall weak, effect of OK on BL raised questions about the differences that might exist when tests of the model are conducted on individuals with high objective knowledge and low objective knowledge separately. Thus, the relationship among OK and other constructs within the privacy calculus should be investigated further, particularly in conjunction with efforts to improve the operationalization of the construct.

Finally, future research should examine this model in other cultures. The majority of privacy calculus research had originated in the United States. This research was set in a Canadian context, which maintains a distinct regulatory environment and was argued to be culturally distinct. Despite the differences, in a global context these two cultural environments are still similar and represent 'WEIRD' societal contexts. It is possible that the results of this study will not be generalizable to more diverse cultures. Therefore, tests of privacy literacy, trust in various stakeholder groups and communication boundary coordination need be undertaken in various contexts.

Implications for Government

The results related to objective knowledge provided insights that can be used by government. Specifically, the objective knowledge items were derived directly from the Office of the Privacy Commissioner (OPC) of Canada and based upon the omnibus privacy legislation, *PIPEDA*, that was enacted to protect individuals in all their information dealings with business in that country. The original items were structured by the OPC in quiz format and represented topics that the OPC had determined most Canadians should know with respect to their information privacy.

It stands to reason that the Office of the Privacy Commissioner of Canada should be particularly interested in the results of this study. Notably, findings indicated that respondents were not well informed about privacy issues or the protections afforded by *PIPEDA*. Although *PIPEDA* is applicable to all businesses conducting personal information transactions with Canadians, the onus to identify and report privacy breaches or other privacy violations remains with the individual. Thus, knowledge of *PIPEDA* is critical to the effectiveness of the protections offered under the *Act*. As this study revealed many areas in which a majority of respondents had inaccurate information, there are clear implications to government. Specifically, a suggestion from this research is that the OPC employ improved citizen education of the *Act* and individuals' commensurate roles and responsibilities.

In addition, results clearly established that privacy concerns among respondents were pronounced. Since the purpose of *PIPEDA* is to protect Canadians from privacy vulnerability, it is reasonable to think that individuals confident they are protected would feel less concern about privacy. Yet, the high level of privacy concern noted in the results suggested that respondents did not have such reassurance. This situation could be due to the poor knowledge of *PIPEDA* previously identified and therefore easily rectified with educational campaigns.

Moreover, new global electronic information exchange platforms such as OSNs constitute complex territory in which to protect citizen information privacy as data frequently crosses national borders or is collected by foreign entities and may be more vulnerable to privacy violations. Therefore, the insight into how individuals navigate their information disclosure decisions in these environments provides important information for regulatory bodies charged with protecting individuals. For, understanding individuals' attitudes and behaviours creates an opportunity to understand the legal protections currently offered and how they might be improved or better communicated.

Finally, even though the results of this study were applicable solely to the Canadian context, numerous governments around the world have privacy legislation similar to that in Canada developed from recommendations from the OECD. Though the specifics of national privacy legislation will differ, those with regulations rooted in OECD's seven principles for protecting individual personal privacy have committed to ensuring its citizens receive notice that data collection will occur, be informed of its clear purpose and offered disclosure, provide consent, be assured of data security and accountability from the collector and be entitled access to their information (OECD, 2011). Therefore, that a reliable and valid instrument of objective privacy knowledge was shown capable of representing privacy legislation should be relevant to governments globally as similar measures could realistically be derived for other legislative environments. Further, where notice and information disclosure are such prominent elements of OECD's recommendations, governments, including Canada, could use objective knowledge scores as one indicator of the effectiveness of privacy regulation. For, if legislation requires informed consent and citizens are unaware of the protections afforded by the legislation, one may argue that more work would be required to ensure compliance.

Implications for Management

Results revealed that trust in the OSN provider was critical to the linkages established in OSNs. As discussed in Section 7.2.3, the manifest items representing boundary linkages included interpersonal and organisational connections engaged in by participants. Specifically, one item measured connections with application providers and another measured connections with external websites. Since most OSNs generate revenue through these external third parties, ensuring participants maximize their connections within the provider's OSN environment should be critical to the business model of those companies. And, since the results of this study suggested that connections can be positively influenced by the trust in the provider, OSN providers should pay particular attention to the trust it has established from participants. Furthermore, the descriptive results of this study showed that trust in the provider was lower than each of the other two types of trust (trust in close connections and trust in all members). Thus, implied in this conclusion is an opportunity for companies to investigate ways to increase trust from participants.

The discussion presented in Section 7.2.3 also indicated that in practice, OSN providers must be able to achieve a balance between satisfying their organisational partners (i.e., advertisers) while also keeping their members happy. As we know that relationship maintenance is generally asserted to be critical to long term profitability (Grönroos, 1994; Schoenbachler and Gordon, 2002) and trust is essential for relationship maintenance (Moorman, Zaltman and Deshpande, 1993; Campbell, 1997; Milne and Boza, 1999), emphasis on trust maintenance and development could also have positive financial implications for OSN providers from this perspective as well. However, as was illustrated in Chapter 7, there are sometimes instances when the privacy interests of member participants conflict with the organisational goals of partner companies and therefore balancing competing interests becomes necessary. Although favouring the revenue stream (i.e. advertisers) in conflicting situations may offer a short term solution, results of this study have clearly established the importance of organisational trust to the OSNs membership. Thus, where the literature maintained that protection of organisational trust was important for long term profitability (Grönroos, 1994; Schoenbachler and Gordon, 2002) and organisational trust by way of boundary linkages was also defended as being critical to an OSN provider's revenue stream (Section 7.2.3), it would appear that choosing to protect the trust held with members would offer a stronger solution with a long term view.

Results of this study also indicated that OSN providers might be encouraged to concentrate upon the objective privacy knowledge findings of this study as a possible way to engender trust with members. Given the low objective privacy knowledge scores observed, OSN providers need to question their responsibility to inform participants about the privacy responsibilities associated with the site and the ways in which member participants are educated about privacy knowledge. Providing a privacy policy is likely insufficient since few people take the time to read them (BusinessWire, 2010; Lawler, Molluzzo and Doshi, 2012; Winkler, 2001) or fail to read them thoroughly (Office of National Statistics, 2011), possibly because the length and complexity of many online privacy policies requires patience most consumers do not have (Krashinsky and El Akkad, 2010). Indeed, many OSN providers might argue that the provision of the company's privacy policy constitutes sufficient effort to educate consumers about the personal information that is being collected and how it is managed. And, while it may be contended that forcing individuals to read the policy is not the responsibility of the organisation, there are likely positive implications of a well-informed usership that could interest OSN providers in emphasising privacy knowledge.

Of course, practitioners should also be prudent about the effect of objective knowledge on privacy linkages within OSNs. It was argued herein that boundary linkages were critical to the financial well-being of the OSN provider but results also showed that increased objective knowledge could restrict boundary linkages. While it might appear that suggestions to concentrate on trust building to prompt linkages and thus financial strength contradicts the intent of emphasis on user privacy knowledge, it is argued that emphasis on objective knowledge results might also serve to increase trust and the related financial benefits. Specifically, if OSN members know the rules about their private information within the network, instances of boundary turbulence would be limited. Boundary turbulence occurs when violations of privacy have occurred or are perceived to have occurred (Petronio, 2002) and organisational trust may be lost (Morgan and Hunt, 1994). In instances inciting public outrage over privacy infringements such as the cases of Facebook Beacon and the Whopper sacrifice, no violation of Facebook's privacy policy had actually occurred, but the perception that violations had occurred prompted intense negative reactions by many members. Thus, OSN providers should consider increasing the privacy knowledge of members as a mechanism to avoid boundary turbulence and protect its trust.

8.4 Concluding Remarks

This study offered a number of important contributions with implications to the science of marketing, business practitioners and governments. Over all, a novel privacy calculus model was offered as a possibile explanation of the privacy paradox.

Specifically, results of this study confirmed a valid and reliable instrument for measuring privacy concern which should help to alleviate some of the contention over its measurement to permit closer comparisons of future research. Second, Communication Privacy Management by way of boundary linkage and permeability coordination processes was evidenced to provide an appropriate explanation of privacy related behaviours within online social networks. Privacy literacy was determined to influence CPM by privacy knowledge accuracy restricting the connections made but privacy knowledge confidence was shown able to overcome that negative influence and permit OSN linkages and information disclosure. Both interpersonal and organisational trust were found to be essential to the explanation of communication privacy management. However, interpersonal trust explained information disclosure directly whereas organisational trust predicted the connections that were made on OSNs. Interestingly, despite privacy concern being observed to be extremely high, the influences of privacy confidence and trust were stronger influences upon privacy management rules within OSNs with this sample.

There were several limitations to this study that required caution in interpretation of findings and presented opportunities for future research. One important limitation was the narrow focus of the research model that intentionally excluded known influences in the privacy calculus in the interest of parsimony. The generalizability of results was also limited due to the snowball technique of data collection employed which may have introduced similarity bias and emphasis on omnibus Canadian legislation in the measure of objective knowledge prevented generalizability of results to other regulatory environments. Methodological limitations pertaining to the philosophical consistency of the research design were also identified with this research, though it was believed that this potential limit had been adequately addressed. Moreover, researcher expertise in conducting focus groups was recognised as a greater study limitation. Lastly, some further caution in interpreting results of this study was required due to the non-normal statistical properties of the privacy concern measure.

Despite the identified limitations, results of this study have also provided a number of opportunities for future research. Namely, as this study emphasised model development with the incorporation of many untested constructs, a need for future research to validate these findings with confirmatory analytic techniques has been created. Also, opportunities to improve upon measures of Communication Privacy Management and objective knowledge were also highlighted. Furthermore, results suggested that there is an opportunity for future research to explore objective knowledge more intensely by investigating alternate measures or examining the differences that might exist within the privacy calculus model through comparison of tests of individuals with high objective knowledge and low objective knowledge. While a substantial amount of the variance in boundary permeability was explained with this model, this research did not attempt to produce an exhaustive explanation of the privacy calculus. Therefore, there is an opportunity for future research to incorporate other previously tested influences within the privacy calculus to provide a more complete understanding of the privacy calculus mechanism. Finally, there are numerous opportunities to extend the research in other cultures and contexts given the contextual nature of most of the constructs under investigation.

Clearly, the implications for the science of marketing included all of the opportunities just identified to improve and extend the understanding of the privacy calculus both within the context of OSNs and outside it. Results of the study also highlighted implications to government and business. Specifically, the low objective knowledge results should be a concern for government and therefore education programs to address the deficiency should be explored. And, the results of this study also suggested that other nations using privacy legislation modelled after OECD recommendations could develop, test and monitor objective knowledge of citizens in order to identify what, if any, action might be required to address knowledge gaps. Finally, results suggested a critical implication for business would be to maintain and enhance trust from its members in order to protect revenue streams. To that end, the importance of OSN providers taking increased responsibility for consumer privacy education was also justified.

References

Acquisti, A. and Gross, R., 2006. Imagined communities: Awareness, information sharing, and privacy on the Facebook. *PET 2006*, Accessed from: <http://privacy.cs.cmu.edu/dataprivacy/projects/facebook/facebook2.pdf>

Acquisti, A. and Gross, R., 2009. Predicting social security numbers from public data. *Proceedings of the National Academy of Science*, 106(27), 10975-10980.

Acquisti, A. and Grossklags, J., 2005. Privacy and rationality in consumer decision making. *IEEE Security and Privacy*, 24-30. Accessed from: <http://csis.pace.edu/~ctappert/dps/d861-09/team2-3.pdf.>.[Accessed July 12, 2011]

Adams, J., Khan, H.T.A., and Raeside, R., 2007. *Research methods for graduate business and social science*, New Delhi, India: Sage.

Adams, M., 2003. *Fire and ice: United States, Canada and the myth of converging values*. Toronto: Penguin Group Canada.

Adler, P., Kwon, S.-W., 2002. Social capital: prospects for a new concept. *Academy of Management Review*, 27(1), pp.17-40.

Alhabeeb, M.J., 2007. Consumer knowledge and consumption: a human capital model. *Academy of Marketing Studies Journal*, 11(1), pp.69-81.

Allen, A. L., 1988. *Uneasy access: privacy for women in a free society*. Rowman and Littlefield Pub Incorporated.

Altman, I., Taylor, D.A., 1973. *Social penetration: the development of interpersonal relationships*. New York: Holt, Rinehart and Winston.

Archer-Brown, C., Piercy, N. and Joinson, A., 2013. Examining the information value of virtual communities: Factual versus opinion-based message content. *Journal of Marketing Management*, 29(3-4), pp.421-438.

Armitage, C. J., Conner, M. 1999. The theory of planned behavior: assessment of predictive validity and 'perceived control'. *British Journal of Social Psychology*, 38(1), pp.35-54.

Arthur, C., 2012. Twitter now has 10m users in UK. *The Guardian*, [online]15 May, Accessed from: <http://www.guardian.co.uk/technology/2012/may/15/twitter-uk-users-10m>. [Accessed from June 19, 2012]

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

Azjen, I., Driver, B. L. 1991. Prediction of leisure participation from behavioral, normative, and control beliefs: an application of the theory of planned behavior. *Leisure Sciences* 13(3), pp.185-204.

Babin, B.J., Hair, J.F. and Bole, J.S., 2008. Publishing research in marketing journals using structural equation modeling. *Journal of Marketing Theory and Practice*, 16(4), pp.141-169.

Baker, W., 1990. Market networks and corporate behavior. *American Journal of Sociology*, 96, pp.589-625.

Barnes, J. A., 1954. Class and committees in a Norwegian island parish. *Human Relations*, (7): pp.39-58.

Bauer, R. A., 1960. Consumer behaviour and risk taking. In R. Hancock (ed.). *Dynamic Marketing for a changing world*. Chicago: AMA. pp.389-398

Beer, D., 2008. Social networking sites…revisiting the story so far: a response to Danah Boyd and Nicole Ellison. *Journal of Computer-Mediated Communication*, 13(2), pp. 516-529.

Bellman, S., Johnson, E.J., Kobrin, S.J., and Lohse, G.L. 2004. International differences in information privacy concerns: a global survey of consumers. *Information Society*, 20, pp. 313-324.

Berendt, B., Oliver, G., and Spiekermann, S., 2005. Privacy in e-commerce: stated preferences vs. actual behavior. *Communications of the ARCH*, 48(40), pp.101-06

Berg, J.H., Clark, M.S., 1986. Differences in social exchange between intimate and other relationships: gradually evolving or quickly apparent? In: V. J. Derlega and B. A. Winstead (Eds.). *Friendship and social interaction.* New York:Springer. Pp.101-128

Berg, J. H., Derlega, V. J., 1987. *Self-disclosure: theory, research, and therapy*. Springer.

Berg, J., Dickhaut, J. and McCabe, K., 1995. Trust, reciprocity and social history. *Games and Economic Behavior*, 10, pp.122-142.

Best, S.J. and Kreuger, B.S., 2006. Online interactions and social capital: distinguishing between new and existing ties. *Social Science and Computer Review*, 24(4), pp. 395 – 410.

Beye, M., Jeckmans, A., Erkin, Z., Hartel, P., Lagendijk, R. and Tang, Q., 2010. *Literature Overview - Privacy in Online Social Networks.* University of Twente, Centre for Telematics and Information Technology, [Internal Report], Accessed from: <http://doc.utwente.nl/74094/1/literaturereview.pdf>. [Accessed May 16, 2012]

Blanchard, A. and Horan, T., 1998. Virtual communities and social capital. *Social Science and Computer Review*, 16(3), pp. 293 - 307.

Blau, P. M., 1964. *Exchange and power in social life*. Transaction Publishers.

Bourdieu, P., 1986. The forms of social capital. In: J. Richardson (ed.). *Handbook of Theory and Rsearch for the Sociology of Education*, pp. 241-58. New York: Greenwood Press.

Boyd, B. K., Gove, S. and Hitt, M. A., 2005. Consequences of measurement problems in strategic management research: the case of Amihud and Lev. *Strategic Management Journal*, 26, pp.367-375.

Boyd, D., 2007. Why youth heart social network sites: the role of networked publics in teenage social life. *The Berkman Center for Internet and Society Research Publication Series, Harvard University*, 16, pp.119-142.

Boyd, D. M., Ellison, N. B., 2007. Social network sites: definition, history, and scholarship. *Journal of Computer-Mediated Communication*, [online] *13*(1), Article 11, pp. 210-230. Accessed from: <http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html>. [Accessed January 7, 2011]

Brown, J., Broderick, A.J., and Lee, N., 2007. Word of mouth communication within online communities: conceptualizing the online social network. *Journal of Interactive Marketing*, [online] 21(3), pp.2-20, DOI:10.1002/dir.20082.

Brucks, M., 1985. The effects of product class knowledge on information search behavior. *Journal of Consumer Research*, 12(June), pp.1-16.

Bryman, A., Teevan, J.T., and Bell, E., 2009. *Social research methods, 2nd Canadian edition*. Toronto, Canada: Oxford University Press.

Bryman, A., 2006. Integrating quantitative and qualitative research: how is it done? *Qualitative Research*, 6, pp. 97-113.

Bryman, A. and Bell, E., 2003. *Business research methods.* New York: Oxford University Press.

Brynner, J., 2006. *The Sage dictionary of social research methods*. Jupp, V. ed. London: Sage Publications.

Buchanan, T., Paine, C., Joinson, N. and Reips, U.D., 2007. Development of measures of online privacy concern and protection for use on the internet. *Journal of the American Society for Information Science and Technology*, 58(2), pp.157-165.

Burgoon, J.K., Parrott, R., LePoire, B.A., Kelley, D.L., Walther, J.B. and Perry, D., 1989. Maintaining and restoring privacy through communication in different types of relationships, *Journal of Social and Personal Relationships*, 6, pp.131-158

Burt, R.S., 1992. *Structural holes: the social structure of competition*. Cambridge, MA: Harvard University Press.

BusinessWire, 2010., The truth about social media identity theft: perception versus reality. *Business Wire*, [online]21 June. Accessed from: <http://www.businesswire.com/news/home/20100621005370/en/Truth-Social-Media-Identity-Theft-Perception-Reality.> [Accessed June 29, 2012]

Campbell, A. (1997). Relationship marketing in consumer markets: a comparison of managerial and consumer attitudes about information privacy. *Journal of Direct Marketing*, 11, pp. 44-58.

Cardon, P.W., Marshall, B., Norris, D.T., Cho, J., Choi, J., Cui, L., Collier, C., El-Shinnaway, M., Goreva, N., Nillson, S., North, M., Raungpaka, V., Ravid, G., Svensson, L., Usluata, A., Valenuala, J.P., Wang, S., and Whelan, C., 2009. Online and offline social ties of social network website users: an exploratory study in eleven societies. *Journal of Computer Information Systems*, 50(1), pp.54-64.

Carlson, J.P., Bearden, W.O., and Hardesty, D.M., 2007. Influences on what consumers know and what they think they know regarding marketer pricing tactics. *Psychology & Marketing*, 24(2), pp. 117-142.

Casteñeda, J.A., Montoso, F.J., and Luque, T., 2007. The dimensionality of customer privacy concern on the internet. *Online Information Review*, 31(4), pp.420-439.

Cavoukian, A. and Cameron, K., 2011. Wi-Fi positioning systems: beware of unintended consequences. [online] Accessed from http://www.ipc.on.ca/images/Resources/wi-fi.pdf. [Accessed July 28, 2013]

Cavoukian, A. and Hamilton, T.J., 2002. *The privacy payoff: how successful businesses build customer trust*. Toronto ON: McGraw-Hill Ryerson

Cespedes, F., and Smith, H., 1993. Database marketing: new rules for policy and marketing. *Sloan management Review*, 35, pp.7-22.

Chao, L., 2011. Renren changes key user figure before IPO. *The Wall Street Journal* [online] 29 April. Accessed from: http://online.wsj.com/article/SB10001424052748704729304576286903217555660.html#ixzz1KqsoJPb8. [Accessed June 19, 2012]

Chartrand, T.L., 2005. The role of conscious awareness in consumer behavior. *Journal of Consumer Psychology*, 15(3), pp.203-210.

Chellappa, R. K., Sin, R. G., 2005. Personalization versus privacy: an empirical examination of the online consumer’s dilemma. *Information Technology and Management*, 6(2-3), pp.181-202.

Cheung, C. M. K., and Lee, M. K. O., 2009. Understanding the sustainability of a virtual community: Model development and empirical test. *Journal of Information Science*, 35(3), pp.279–298.

Cheung, C.M.K., Chiu, P.Y., and Lee, M.K.O., 2010. A theoretical model of intentional social action in online social networks. *Decision Support Systems*, 49, pp.24-30.

Cheung, C.M.K., Chiu, P.Y., and Lee, M.K.O., 2011. Online social networks: why do students use Facebook? *Computers in Human Behavior*, 27, pp.1337-1343.

Child, J., Pearson, J.C. and Petronio, S., 2009. Blogging, communication, and privacy management: Development of the blogging privacy management measure. *Journal of the American Society for Information Science and Technology*, 60(10), pp.2079-2094.

Child, J.T. and Petronio, S., 2011. Unpacking the paradoxes of privacy in CMC relationships: the challenges of blogging and relational communication on the Internet. In Wright, K.B. and Webb, L.M. eds., 2011. *Computer mediated communication in personal relationships*. New York: Peter Lang Publishing Inc. Ch. 2.

Chiu, C.M., Hsu, M.H., and Wang, E.T.G., 2006. Understanding knowledge sharing in virtual communities: an integration of social capital and social cognitive theories. *Decision Support Systems*, 42, pp. 1872 – 1888.

Chong, L. and Gibbons, P., 1997. Corporate entrepreneurship: the roles of ideology and social capital, *Group and Organizational Management*, 22, pp.10-30.

Christofides, E., Muise, A., and Desmarais, S., 2009. Information disclosure and control on Facebook: are they two sides of the same coin or different processes? *CyberPsychology and Behavior*, 12(3), pp.341-345

Coffé, H. and Geys, B., 2007. Toward an empirical characterization of bridging and bonding social capital. *Nonprofit and Voluntary Sector Quarterly*, 36, pp.121-139.

Cohen, J. E., 2000. Examined lives: informational privacy and the subject as object. *Stanford Law Review*, pp.1373-1438.

Cole, C.A., Gaeth, G. and Singh, S.N., 1986. Measuring prior knowledge. *NA - Advances in Consumer Research*, 13, pp. 64-66.

Coleman, J.S., 1988. Social capital in the creation of human capital. *American Journal of Sociology*, 94, Supplement: Organizations and Institutions: Sociological and Economic Approaches to the Analysis of Social Structure, pp.S95-S120.

Collins, N.L. and Miller, L.C., 1994. Self-disclosure and liking: a meta-analytic review. *Psychological Bulletin*, 116, pp.457–474.

Cooper, D. R., and Schindler, P. S., 2003. *Business research methods*. 8th ed. New York: McGraw-Hill.

Cosgrove, C., 2012. Study: social media use plateaus. *The Chronicle Herald*, 6 Jan. p.C4.

Cox, J.C., 2004. How to identify trust and reciprocity. *Games and Economic Behavior*, 46, pp.260-281.

Crabtree, B.F., Yankoshik, M.K., Miller, W.M., and O'Connor, P.J., 1993. Selecting individual or group interviews. *In:* D.L. Morgan (ed.) *Successful Focus Groups*, London: Sage Publications.

Craig, J.D.R., 1997. Invasion of privacy and charter values: the common-law tort awakens. *McGill Law Journal*, 42, pp.355-399

Creswell, J. W., 1994. *Research design: qualitative and quantitative approaches*. London: Sage Publications.

Creswell, J. W., 2009. *Research design: qualitative, quantitative and mixed method approaches*. 3rd ed. Thousand Oaks, CA: Sage Publications.

Creswell, J. W., Plano Clark, V.L., 2011. *Designing and conducting mixed methods research*. 2nd ed. Thousand Oaks, CA: Sage Publications.

Creswell, J. W., Plano Clark, V., Gutmann, M. and Hanson, W., 2003. Advanced mixed methods designs. In: A. Tashakkori and C. Teddle, (Eds.) *Handbook of mixed method research in the social and behavioral sciences*, pp. 209-240, Thousand Oaks, CA: Sage.

Culnan, M.J., 1993. How did they get my name?: an exploratory investigation of consumer attitudes toward secondary use information. *MIS Quarterly*, 17(3), pp.341-361.

Culnan, M.J., 1995. Consumer awareness of name removal procedures: implications for direct marketing. *Journal of Direct Marketing*, 9 (2), pp.10-19,

Culnan, M.J. and Armstrong, P.K., 1999. Information privacy concerns, procedural fairness and impersonal trust: an empirical investigation. *Organizational Science*, 10(1), pp.104-115.

Culnan, M. J., and Bies, R. J., 2003. Consumer privacy: balancing economic and justice considerations. Journal of social issues, 59(2), pp.323-342.

Davidson, J., 2006. *The sage dictionary of social research methods*. Jupp, V. ed., London: Sage Publications.

Dasgupta, P. (2000). Economic progress and the ideal of social capital. In: P. Dasgupta, and I. Serageldin. (Ed). *Social Capital: A Multifaceted Perspective.* The World Bank.

Day, G. and Montgomery, D., 1999. Charting new directions for marketing. *Journal of Marketing*, 63, pp.3-13.

Debatin, B., Lovejoy, J.P., Horn A.K., and Hughes, B.N., 2009. Facebook and online privacy: attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, 15, pp.83-108.

DeCew, J., 1997. *In pursuit of privacy: law, ethics, and the rise of technology.* Ithaca: Cornell University Press.

Dewing, M., 2010. *Social media: who uses them?* Library of Parliament background paper, (Publication No. 2010-05-E). Canada: Parliamentary Information and Research Service.

Dholakia, U.M., Bagozzi, R.P. and Pearo, L.K., 2004. A social influence model of consumer participation in network- and small-group-based virtual communities. *International Journal of Research in Marketing*, 21(3), pp.241–263.

Dinev, T. and Hart, P., 2004. Internet privacy concerns and their antecedents: measurement validity and regression model. *Behaviour and Information Technology*, 23(6), pp.413-422.

Dinev, T. and Hart, P., 2006a. Privacy concerns and levels of information exchange: an empirical investigation of intended e-services use. *e-Service Journal*, pp.25-59.

Dinev, T. and Hart, P., 2006b. An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1), pp.61-80.

Dinev, T. and Hart, P., 2006c. Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce*, 10(2), pp.7-29.

Direct Marketing Association, 2012. Data privacy: what the consumer really thinks 2012. *The Direct Marketing Association (UK) Ltd*. Accessed from: http://dma.org.uk/sites/default/files/tookit_files/data_privacy_-_what_the_consumer_really_thinks_2012.pdf [Accessed June 10, 2013]

Donaldson, T. and Dunfee, T.W., 1994. Toward a unified conception of business ethics: integrative social contracts theory. *Academy of Management Review,*19(2) pp.252-284.

D'Souza, G. and Phelps, J.E., 2009. The privacy paradox: the case of secondary disclosure. *The Berkeley Electronic Press*, 7(4).

Dunne, Á., Lawlor, M.A. and Rowley, J., 2010. Young people's use of online social networking sites: a uses and gratifications perspective. *Journal of Research in Interactive Marketing,* 4(1), pp. 46-58.

Dwyer, C., Hiltz, S. R., and Passerini, K., 2007. Trust and privacy concern within social networking sites: a comparison of Facebook and MySpace. In: *Proceedings of AMCIS*, 2007(Aug).

Eastlick, M.A., Lotz, S.L. and Warrington, P., 2006. Understanding online B-to-C relationships: an integrated model of privacy concerns, trust, and commitment. *Journal of Business Research*, 59, pp.877-886.

Echambadi, R., Campbell, B., and Agarwal, R., 2006. Encouraging best practice in quantitative management research: an incomplete list of opportunities. *Journal of Management Studies*, 43(8), pp.801-20.

Edwards, B. and Foley,M., 1997. Social capital and the political economy of our discontent. *American Behavioral Scientist*, 40(5), pp. 669-678.

Ellen, P.S., 1994. Do we know what we need to know? Objective and subjective knowledge effects on pro-ecological behaviors. *Journal of Business Research*, 30(1), pp.43-52.

Ellison, N.B., Steinfield, C. and Lampe, C., 2007. The benefits of Facebook 'friends': social capital and college students' use of online social network sites. *Journal of Computer-Mediated Communication*, 12(4), pp.1143-1168.

eMarketer, 2012. Facebook helps get one in five people worldwide socializing on online networks. [online]15 March, Accessed from <http://www.emarketer.com/Article.aspx?R=1008903> [Accessed March 15, 2012]

Emerson, R. M., 1962. Power-dependence relations. *American Sociological Review*, 27, pp.31–40.

Experian Hitwise, 2012. Top 20 sites and engines. [online]5 May, Accessed from: <http://www.hitwise.com/ca/datacenter/main/dashboard-10557.html> [Accessed May 8, 2012]

Faase, R., Helms, R. and Spruit, M., 2011. Web 2.0 in the CRM domain: Defining social CRM. *International Journal of Electronic Customer Relationship Management*, 5(1), pp.1-22.

Falk, R.F. and Miller, N.B., 1992. *A primer for soft modelling*. Akron, OH: The University of Akron Press.

Faulkner, P., 2010. Norms of trust, Millar and Pritchard (eds). *Social Epistemology*, OUP: 2010

Ferguson, C.J., 2009. An effect size primer: a guide for clinicians and researchers. *Professional Psychology: Research and Practice*, 40(5), pp.532-538.

Field, A., 2005. *Discovering statistics using SPSS*. 2nd ed. London: Sage Publications

Floridi, L., 2006. Ontological interpretation of informational privacy, ethics and information technology. 1–16 DOI 10.1007/s10676-006-0001-7

Foxman, E. R. and Kilcoyne, P., 1993. Information technology, marketing practice, and consumer privacy: ethical issues. *Journal of Public Policy and Marketing*, 12(1), pp.106-119.

Fried, C., 1970*, An anatomy of values,* Cambridge: Harvard University Press.

Fried, C., 1984. Privacy. In: F. D. Schoeman (Ed.). *Philosophical dimensions of privacy*, New York: Cambridge University Press. pp.203-222

Fukuyama, F., 1995. *Trust: the social virtues and the creation of prosperity*. New York, NY: Free Press.

Fuller, T.D., Edwards, J.N., Vorakitphokatorn, S. and Sermsri, S., 1993. Using focus groups to adapt survey instruments to new populations: experience from a developing country. In: *Successful Focus Groups.* D.L. Morgan (ed.) London: Sage.

Ganesan, S., 1994. Determinants of long-term orientation in buyer-seller relationships. *Journal of Marketing, 58*, pp.1-19.

Gabarino, E., and Johnson, M. S., 1999. The different roles of satisfaction, trust, and commitment in customer relationships. *The Journal of Marketing*, pp.70-87.

Garton, C.L., and Haythornthwaite, B.W. and Wellman, B., 1997. Studying online social networks. *Journal of Computer-Mediated Communication*, [online] 3(1), Accessed from: <http://onlinelibrary.wiley.com.libproxy.stfx.ca/doi/10.1111/j.1083-6101.1997.tb00062.x/full> [Accessed August 29, 2011]

Gauthier, D., 2011. Follow up: the Canadian twitterer. *Little Fish Big Pond with Danielle Gauthier*, [online]6 May, Accessed from: <http://daniellegauthier.com/2011/05/canadian-twitter-usage/> [Accessed June 19, 2012]

Geromel, R., 2011. Facebook surpasses Orkut, owned by Google, in numbers of users in Brazil. *Forbes*, [online]14 September. Accessed from: <http://www.forbes.com/sites/ricardogeromel/2011/09/14/facebook-surpasses-orkut-owned-by-google-in-numbers-of-users-in-brazil/> [Accessed May 8, 2012]

Gjoka, M., Kurant, M., Butts, C.T., and Markpoulou, A., 2011. A walk in Facebook: uniform sampling of users in online social networks. *IEEE Journal on Selected Areas in Communications (JSAC)*, Special Issue on Measurement of Internet Topologies.

Golembiewski, R. T., and McConkie, M., 1975. The centrality of interpersonal trust in group processes. *Theories of group processes,* 131, p.185.

Goodwin, C., 1991. Privacy: recognition of a consumer right. *Journal of Public Policy and Marketing*. 10(1), pp.149-166.

Govani, T. and Pashley, H., 2005. Student awareness of the privacy implications when using Facebook. [online] Accessed from: <http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf> [Accessed May 12, 2012]

Grabner-Kräuter, S. and Kaluscha, E.A., 2003. Empirical research in on-line trust: a review and critical assessment. *International Journal of Human-Computer Studies*, 58, pp.783-812.

Graeff, T.R. and Harmon, S., 2002. Collecting and using personal data: consumers' awareness and concerns. *Journal of Consumer Marketing*, 19(4), pp.302 – 318.

Granovetter, M.S., 1973. The strength of weak ties. *American Journal of Sociology*, 78(6), pp. 1360-1380.

Granovetter, M.S., 1982. The strength of weak ties: a network theory revisited, In P.V. Marsden and N. Lin (Eds.). *Social structure and network analysis*, Thousand Oaks, CA: Sage Publications. pp.105-130

Greene, J.C., Caracelli, V.J. and Graham, W.F., 1989. Toward a conceptual framework for mixed-method evaluation designs. *Educational Evaluation and Policy Analysis*, 11(3), pp. 255-274.

Greenwald, G. and MacAskill, E., 2013. NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*, June 7 [online] Accessed from: < http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data> [Accessed on: July 3, 2013].

Grönroos, C. 1994. Quo vadis marketing? Toward a relationship marketing paradigm. *Journal of Marketing Management*, 10, pp. 347-360.

Gross, R., and Acquisti, A., 2005. Information revelation and privacy in online social networks. *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, pp.71-80, DOI 10.1145/1102199.1102214

Hair, J.F, Black, W.C., Babin, B.J. and Anderson, R.E., 2010. *Multivariate data analysis*. Upper Saddle River, NJ: Prentice Hall.

Hair, J.F., Hult, G.T.M., Ringle, C.M. and Sarstedt, M., 2013. *A primer on partial least squares structural equation modeling (PLS-SEM)*. Los Angeles, CA: Sage.

Hair, J.F., Ringle C,M., and Starstedt, M., 2011. PLS-SEM: indeed a silver bullet. *Journal of Marketing Theory and Practice*, 19(20) pp.130-151.

Hann, I.-H., Hui, K.-L., Lee. T.S., and Png, I.P.L., 2002. Online information privacy: measuring the cost-benefit trade-off. *Proceedings of the Twenty Third International Conference on Information Systems,* 10 pages.

Hann, I.-H., Hui, K.-L., Lee. T.S., and Png, I.P.L., 2007. Overcoming online information privacy concerns: an information-processing theory approach. *Journal of Management Information Systems* 24(2), pp.13–42.

Hargittai, E., 2008. The participation divide: content creation and sharing in the digital age. *Information, Communication and Society*, 11(2), pp.239-256.

Harris Decima, 2011. 2011 Canadians and privacy survey. *presented to the Office of the Privacy Commissioner of Canada*,[online]31 March. Accessed from: <http://www.priv.gc.ca/information/por-rop/2011/por_2011_01_e.pdf> [Accessed August 25, 2011]

Hart, C., Johnson, M., 1999. Growing the trust relationship. *Marketing Management* 8 (1) pp.8–19.[47]

Hart, J., Ridley, C., Taher, F., Sas, C. and Dix, A., 2008. Exploring the Facebook experience: a new approach to usability. In: *NordiCHI 2008: Using Bridges*, Lund, October 18-22.

Haythornthwaite, C., 2005. Social networks and internet connectivity effects. *Internet Communication and Society*, 8(2), pp. 125-147.

Henrich, J., Heine, S. J., and Norenzayan, A., 2010. Most people are not WEIRD. *Nature*, 466(7302), pp.29-29.

Henry, G.T., 1990. *Practical sampling, Applied Social Research Methods, Volume 21*, Newbury Park, California: Sage Publications.

Hilton, B.A., Budgen, C., Molzahn, A.E. and Attridge,C.B., 2001. Developing and testing instruments to measure client outcomes at the Comox Valley Nursing Center. *Public Health Nursing*, 18(5), pp. 327-339.

Hoadley, C. M.; Xu, H., Lee, J. J., Rosson, M. B., 2010. Privacy as information access and illusory control: the case of the Facebook news feed privacy outcry.

Electronic Commerce Research and Applications, 9(1), pp.50-60, DOI: 10.1016/j.elerap.2009.05.001; (*AN 47610937*)

Hoffman, D. L., Novak, T. P., and Peralta, M. A., 1999. Information privacy in the marketspace: implications for the commercial uses of anonymity on the web. *The Information Society*, 15(2), pp.129-139.

Hoofnagle, C. J., King, J., Li, S. and Turow, J., 2010. How different are young adults from older adults when it comes to information privacy attitudes and policies? [online], Available at SSRN: http://ssrn.com/abstract=1589864 or http://dx.doi.org/10.2139/ssrn.1589864

Houghton, D., Joinson, A., Caldwell, N. and Marder, B., 2013. Tagger's delight? Disclosure and liking behavior in Facebook: the effects of sharing photographs amongst multiple known social circles. *Birmingham Business School Discussion Paper Series*, University of Birmingham.

Huffman, M., 2013. Are you sharing too much information? With Twitter, Facebook and other social media, it's very easy to do. *Consumer Affairs*, January 8, Accessed August 1, 2013 from http://www.consumeraffairs.com/news/are-you-sharing-too-much-information-080113.html.

Hui, K. L., Tan, B. C., and Goh, C. Y., 2006. Online information disclosure: motivators and measurements. *ACM Transactions on Internet Technology (TOIT*), 6(4), pp.415-441.

Introna, L.D. and Pouloudi, A., 1999. Privacy in the information age: stakeholders, interests and values. *Journal of Business Ethics*, 22, pp.27-38.

Ipsos, 2011. Canada's love affair with online social networking continues. *Ipsos.com*, [online]14 July. Accessed from: <www.ipsos-na.com/news-polls/pressrelease.aspx?id=5286> [Accessed January 20, 2012]

Ipsos Reid (2009). What? You don't have a social network profile? You are now in the minority. June 19, 2009.

Ipsos Reid, 2011. Ipsos Canadian Inter@ctive Reid Report: 2011 Fact Guide, March 29, 2011.

Johnson, B., 2010. Privacy no longer a social norm, says Facebook founder. *The Guardian*, [online]11 January. Accessed from: <www.guardian.co.uk>

Johnson, L.G. and Sabin, K., 2010. Sampling hard-to-reach populations with respondent sampling. *Methodological Innovations Online* 5(2), pp.38-48

Joinson, A., 2008. 'Looking at', 'looking up' or 'keeping up with' people? Motives and uses of Facebook. In: CHI 2008 Proceedings, *CHI 2008*, Florence, Italy, 5-10 April 2008.

Joinson, A. N. and Paine, C.B., 2007. Self-disclosure, privacy and the Internet. In Joinson, McKenna, Postmes and Reips (Eds.), *Oxford Handbook of Internet Psychology*, Oxford: Oxford University Press, pp. 237-252.

Joinson, A.N., Paine, C., Reips, U.-D., Buchanan, T., 2010. Privacy, trust and self-disclosure online. *Human-Computer Interaction*, 25, pp.1-24.

Kapoor, H., 2009. Focus on trust in marketing scholarship and practice: an historical perspective. In: ASAC, Administrative Sciences Association of Canada, *37th Annual Conference on Creating Knowledge in the New Economy*, Niagara Falls, Ontario, 6-9 June 2009.

Kazeniak, A., 2009. Social networks: Facebook takes over top spot, twitter climbs. [online], Accessed from: <https://blog.compete.com/2009/02/09/facebook-myspace-twitter-social-network/> [Accessed August 25, 2011]

Keaney, A., 2009. Identity theft and privacy–consumer awareness in Ireland. *International Journal of Networking and Virtual Organisations*, 6(6), pp.620-633.

Keen, A., 2012. Andrew Keen: society isn't a startup and sharing's not caring. *Wired.co.uk*. [online]3 May 3Accessed from: http://www.wired.co.uk/magazine/archive/2012/06/ideas-bank/society-isnt-a-startup> [Accessed May 7, 2012]

Kemper, E.A., Stringfield, S., and Teddlie, C., 2003. Mixed methods sampling strategies in social science research. In: Tashakkori, A. and Teddlie, C. (eds.). *Handbook of Mixed Methods in Social and Behavioral Research*, Thousand Oaks, CA: Sage Publications.

Kim, D., 2008. Self-perception-based versus transference-based trust determinants in computer-mediated transactions: a cross-cultural comparison study. *Journal of Management Information Systems* 24 (4) (Spring 2008) pp.13–45.

Kinnear, T.C. and Taylor, J.R., 1996. *Marketing research: an applied approach*. 5th ed. New York: McGraw-Hill Inc.

Kosinski, Stillwell, D. and Graepel, T., 2013. Private traits and attributes are predictable from
digital records of human behavior. *Proceedings of the National Academy of Sciences (PNAS) of the United States of America*, 11 March, 2013. Accessed from: http://www.pnas.org/content/early/2013/03/06/1218772110.full.pdf+html [Accessed June 8, 2013]

Krackhardt, D. and Hanson, J.R., 1993. Informal networks: the company behind the chart. *Harvard Business Review*, 71(4), pp.104-111.

Krasavana, M.L., Nusair, K. and Teodosic, K., 2010. Online social networking: redefining the human web. *Journal of Hospitality and Tourism*, 1(1), pp.68-82.

Krashinsky, S. and El Akkad, O., 2010 The End of Online Privacy. *Globe and Mail*, [online]13 August Accessed from: <http://www.theglobeandmail.com/news/technology/the-end-of-online-privacy/article1672466/page3/> [Accessed May 11, 2011]

Krasnova, H. and Veltri, N.F., 2010. Privacy calculus on social networking sites: explorative evidence from Germany and USA. *Proceedings of the 43rd International Conference on System Sciences*, Hawaii, USA.

Krasnova, H., Spiekermann, S., Koroleva, K., and Hildebrand, T., 2010. Online social networks: why we disclose. *Journal of Information Technology*, 25, pp.109-125.

Krasnova, H., Veltri, F., and Günther, O., 2012. Self-disclosure and privacy calculus on social networking sites: the role of culture. *Business and Information Systems Engineering*, 3, pp.127-135.

Kuhn, T.S., 1962. *The structure of scientific revolution*. Chicago: University of Chicago Press

Kumaraguru, P. and Cranor, L.F., 2005. Privacy indexes: a survey of Westin's studies. *Institute for Software Research International*, [online], Accessed from: <http://reports-archive.adm.cs.cmu.edu/anon/isri2005/CMU-ISRI-05-138.pdf> [Accessed August 18, 2011]

Lampe, C., Ellison, N. and Steinfield, C., 2006. A Face(book) in the crowd: social searching vs. social browsing. In: Association for Computing Machinery (ACM), *Computer Supported Cooperative Work (CSCW) Conference*, Banff, AB, Canada, 4-6 November.

Langenderfer, J. and Miyazaki, A. D., 2009. Privacy in the information economy. *Journal of Consumer Affairs*, 43(3), pp.80-388.

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

Lawler, J.P., Molluzzo, J.C. and Doshi, V., 2012. An expanded study of net generation perceptions on privacy and security on social networking sites (SNS). *Information Systems Education Journal*, 10(1), pp.21-36.

Lee, D.H., Im, S. and Taylor, C.R., 2008. Voluntary self-disclosure of information on the Internet: a multi-method study of the motivations and consequences for disclosing information on blogs. *Psychology and Marketing*, 25(7): pp.692–710.

Lenhart, A., 2009. Pew internet project data memo. *Pew Internet and American Life Project*, January 14, 2009.

Leonard, A., 2004. You are who you know. *Salon.com*, [online]15 June, Accessed from: <http://www.salon.com/2004/06/15/social_software_one/> [Accessed May 15, 2012]

Leonard, M., 2004. Bonding and bridging social capital: reflections from Belfast. *Sociology*, 38(5), pp. 927-944.

Lewis, J. D., and Weigert, A., 1985. Trust as a social reality. *Social Forces*, 63(4), pp.967-985.

Li, H., Sarathy, R. and Xu, H., 2010. Understanding situational online information disclosure as a privacy calculus. *Journal of Computer Information Systems*, 51(1), pp.62-71.

Lian, J.W., and Lin, T.M., 2008. Effects of consumer characteristics on their acceptance of online shopping: comparisons among different product types. *Computers in Human Behaviour*, 24, pp.48-65.

Lin, N., 1999. Building a network theory of social capital. *Connections*, 22(1), pp.28-51.

Lin, N., Cook, K., and Burt, R., 2001. *Social capital: theory and research.* NY: Aldine DE Gruyter.

Lin, S.-W. and Liu, Y.-C., 2012. The effects of motivations, trust and privacy concern in social networking. *Service Business*, 6(4), pp. 411-424.

Lipschultz, J.H., 2012. Privacy is dead – really? *Huffington Post*, 28 August, [online] Accessed from: <http://www.huffingtonpost.com/jeremy-harris-lipschultz/online-privacy_b_1831956.html> [Accessed August 31, 2012]

Liu, C., Marchewka, J.T., Lu, J. and Yu, C.S., 2005. Beyond concern – a privacy-trust-behavioral intention model of electronic commerce. *Information and Management*, 42, pp.289-304.

Livingstone, S., 2008. Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media and Society*, 10(3), pp.393-411.

Lohr, S.L., 2010. *Sampling: design and analysis, 2nd edition*. Boston: Brooks/Cole CENGAGE Learning.

Long, G., Hogg, M.K., Hartley, M., and Angold, S., 1999. Relationship marketing and privacy: exploring the thresholds. *Journal of Marketing Practice*, 5(1), p.4.

Luhmann, N., 1979. *Trust and power: two works*. Chichester: Wiley.

Luhmann, N., 1988. Familiarity, confidence, trust: problems and alternative. In: D. Gambetta (Ed). *Trust: making and breaking cooperative relations.* Oxford: Blackwell.

Luo, X., Lib, H., Zhang, J. and Shimd, J.P. 2010. Examining multi-dimensional trust and multi-faceted risk in initial acceptance of emerging technologies: an empirical study of mobile banking services. *Decision Support Systems,* 49(2), pp.222–234.

Lwin, May, Jochen Wirtz, and Williams, J.D., 2007. Consumer online privacy concerns and responses: a power-responsibility equilibrium perspective. *Journal of the Academy of Marketing Science,* 35 (4), p.572 – 585 DOI: 10.1007/s11747-006-0003-

Lyon, D., 1994. *The electronic eye: the rise of surveillance society*. University of Minnesota Press: Minneapolis.

Madden, M., 2010. Older adults and social media, Pew Internet and American Life Project. *Pew Research Center*, August 27, 2010.

Madden, M., 2012. Privacy management on social media sites. *Pew Research Center's Internet and American Life Project,* [online]24 February, Accessed from: <http://pewinternet.org/~/media//Files/Reports/2012/PIP_Privacy_management_on_social_media_sites_022412.pdf> [Accessed July 12, 2012]

Madden, M. and Zickuhr, K., 2011. 65% of online adults use social networking sites, Pew Internet Project SNS Update 2011. *Pew Internet and American Life Project*, [online] Washington, D.C. Accessed from: <http://pewinternet.org/~/media/files/reports/2011/pip-sns-update-2011.pdf>

Malhotra, N.K., 2002. *Basic marketing research: applications to contemporary issues*, Upper Saddle River, NJ: Prentice Hall.

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

Margulis, S.T., 2003. Privacy as a social issue and behavioural concept. *Journal of Social Issues,* 59(2), July, pp.243-261.

Marpsat, M. and Razafindratsima, N., 2010. Survey methods for hard-to-reach populations: Introduction to the special issue. *Methodological Innovations Online,* 5(2) pp.3-16, Accessed from:<http://www.pbs.plym.ac.uk/mi/pdf/05-08z10/2.%20Marpsat%20and%20Razafindratsima%20English2%20(formatted).pdf> [Accessed Nov. 9, 2012]

McCauley, D., and Kuhnert, K., 1992. A theoretical review and empirical investigation of employee trust in management. *Public Administration Quarterly*, 16(Summer), pp. 265-284.

McEvily, B., Perrone, V., and Zaheer, A., 2003. Trust as an organizing principle. *Organization science*, 14(1), pp.91-103.

McKnight, D.H. and Chervany, N.L., 2003. The meanings of trust. MISRC Working Paper, In: Grabner-Kräuter and Kaluscha.

McLain, D. L. and Hackman, K., 1999. Trust, risk and decision-making in organizational change. *Public Administration Quarterly*, Summer, pp.152-176.

McNaughton, M., 2012. Social networking stats: tagged tops 330 million registered users #RLTM scoreboard. *The Real Time Report*, [online]10 February, Accessed from: <http://therealtimereport.com/2012/02/10/social-networking-stats-tagged-tops-330-million-registered-users-rltm-scoreboard/ > [Accessed May 8, 2012]

Meeks, B.N., 2000. Is privacy possible in the digital age? If it isn't dead, then it's hanging on by a thread. *MSNBC*, [online]8 December, Accessed from: <http://www.msnbc.msn.com/id/3078854/t/privacy-possible-digital-age/> [Accessed December 7, 2012]

Metzger, M.J., 2004. Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce. *Journal of Computer-Mediated Communication*, [e-journal] 9(4). Available through St.FX University website <http://onlinelibrary.wiley.com.libproxy.stfx.ca/doi/10.1111/j.1083-6101.2004.tb00292.x/full#f2> [Accessed May 13, 2012].

Metzger, M. J. 2007. Communication privacy management in electronic commerce. *Journal of Computer-Mediated Communication*, [online] *12*(2), article 1. Accessed through <http://jcmc.indiana.edu/vol12/issue2/metzger.html> [Accessed May 13, 2012].

Meyers, L.S., Gamst, G., and Guarine, A.J., 2006. *Applied multivariate research: design and interpretation*. Thousand Oaks, California: Sage Publications Inc.

Meyerson, M., 2010. *Success secrets of the social media marketing superstars*, Canada: Entrepreneur Media Inc.

Midha, V., 2012. Impact of consumer empowerment on online trust: an examination across genders. *Decision Support Systems*, 54(1), pp.198-205.

Milberg, S.J., Smith, H.J., and Burke, S.J., 2000. Information privacy: corporate management and national regulation. *Organization Science*, 11(1), pp. 35-57.

Milne, G. R.,1997. Consumer participation in mailing lists: a field experiment. *Journal of Public Policy and Marketing*, pp.298-309.

Milne, G. R. and Boza, M.E., 1999. Trust and concern in consumers' perceptions of marketing information management practices. *Journal of Interactive Marketing,* 13(1), pp.5-24.

Milne, G. R., and Gordon, M. E., 1993. Direct mail privacy-efficiency trade-offs within an implied social contract framework. *Journal of Public Policy and Marketing*, pp.206-215.

Milne, G. R. and Rohm, A.J., 2000. Consumer privacy name removal across direct marketing channels: exploring opt-in and opt-out alternatives. *Journal of Public Policy and Marketing*, 19(2), pp.238-249.

Milne, G. R. and Culnan, M.J., 2004. Strategies for reducing online privacy risks: why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing*, 18(3), pp.15-29.

Moon, Y.M., 2000. Intimate exchange: using computers to elicit self-disclosure from consumers. *Journal of Consumer Research*, 26, pp.323–339.

Moor, J.H., 1990. The ethics of privacy protection. *Library Trends*, 39(1and2), pp.69-82.

Moore, A.D., 2003. Privacy: its meaning and value. *American Philosophical Quarterly*, 40(3), pp.215-227

Moorman, C., Deshpande, R., and Zaltman, G., 1993. Factors affecting trust in market research relationships. *Journal of Marketing, 57*, pp.81-101.

Moorman, C., Diehl, K., Brinberg, D., and Kidwell, B., 2004. Subjective knowledge, search locations, and consumer choice. *Journal of Consumer Research,* 31(December), pp.673-80.

Morgan, D.L., 2006. *The Sage Dictionary of Social Research Methods*. Jupp, V. ed. London: Sage Publications.

Morgan, D.L. and Krueger, R.A., 1993. When to use focus groups and why. In: *Successful Focus Groups*. D.L. Morgan (ed.) London: Sage Publications.

Morgan, R.M., and Hunt, S.D., 1994. The commitment-trust theory of relationship marketing. *Journal of Marketing*, 58(3), pp. 20-38.

Morrison, B., 2011. Empirical research in consumer information privacy concern online: a review and critical assessment. *Proceedings of 41st ASB Conference*, Charlottetown, PE, Sept 30-Oct 2, 2011.

Moscardelli, D.M. and Divine, R., 2007. Adolescents' concern for privacy when using the internet: an empirical analysis of predictors and relationships with privacy predicting behaviors. *Family and Consumer Sciences Research Journal*, 35(3), pp.232-252.

MSN Money Partner, 2012. Inside Facebook's money machine: the social network's biggest asset is its user base, which generates billions of likes and comments per day. *MSN Money Partner*, May 17, [online] Accessed from: <http://money.msn.com/technology-investment/post.aspx?post=869a1b6c-0bb7-47b3-ac0a-25d10f6a5404> [Accessed June 11, 2013].

Mueller, S., Francis, L. and Lockshin, L., 1998. The relationship between wine liking, subjective and objective wine knowledge: does it matter who is in your 'consumer' sample? *4th International Conference of the Academy of Wine Business Research*, Siena 17-19th July 2008. [online] Accessed from: < http://academyofwinebusiness.com/wp-content/uploads/2010/04/The-relationship-between-wine-liking_paper.pdf> [Accessed on June 24, 2013].

Nahapiet, J. and Ghoshal , S., 1998. Social capital, intellectual capital, and the organizational advantage. *The Academy of Management Review*, 23(2), pp. 242-266.

Nasser, F., and Wisenbaker, J., 2003. A Monte Carlo study investigating the impact of item parceling on measures of fit in confirmatory factor analysis. *Educational and Psychological Measurement*, *63*(5), pp.729-757.

Naughton, J., 2013. NSA surveillance: don't underestimate the extraordinary power of metadata. *The Guardian*: *The Observer*, June 21 [online]. Accessed from: < http://www.guardian.co.uk/technology/2013/jun/21/nsa-surveillance-metadata-content-obama> [Accessed June 22, 2013].

Nehf, James P., 2007. Shopping for privacy on the internet. *Journal of Consumer Affairs*, 41 (Winter), pp.351-365.

Newton, K., 1997. Social capital and democracy. *American Behavioral Scientist,* 40(5), pp. 575-586.

Nicholson, S., 2011. The gender divide: Are men better than women at social networking? *LinkedIn Blog*, [online]22 June, Accessed from: <http://blog.linkedin.com/2011/06/22/men-vs-women/> [Accessed June 19, 2012]

Nissenbaum, H. F., 2010. *Privacy in context: technology, policy, and the integrity of social life*. Stanford Law and Politics.

Nooteboom, B., 2002. *Trust: forms, foundations, functions, failures and figures,* Northampton, MA: Edward Elgar.

Norberg, P.A., Horne, D. R., and Horne, D.A., 2007. The privacy paradox: personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, 41(1), pp.100-126.

Nosko, A., Wood, E., and Molema, S. (2010) All about me: disclosure in online social networking profiles: the case of FACEBOOK. *Computers in Human Behavior*, 26, 406-418.

Nowak, G.J. and Phelps, J., 1992. Understanding privacy concerns: an assessment of consumers' information-related knowledge and beliefs. *Journal of Direct Marketing*, 6(4), pp.28-39.

Nowak, G.J. and Phelps, J., 1995. Direct marketing and the use of individual-level consumer information: determining how and when "privacy" matters. *Journal of Direct Marketing*, 9(3), pp.46-60.

O'Brien, K., 1993. Improving survey questionnaires. In: *Successful Focus Groups.* D.L. Morgan (ed.) London: Sage Publications.

OECD, 2011. The evolving privacy landscape: 30 years after the OECD privacy guidelines. Accessed from: < http://www.oecd.org/internet/ieconomy/47683378.pdf > [Accessed on December 12, 2012]

Ofcom, 2008. Social networking: a quantitative and qualitative research report into attitudes behaviour and use. *Government Office of Communications*, United Kingdom.

Ofcom, 2012a. Adult media use and attitudes report. *Ofcom.org*, Accessed from: <http://stakeholders.ofcom.org.uk/market-data-research/media-literacy/archive/medlitpub/medlitpubrss/adults-media-use-attitudes/> [Accessed June 18, 2012]

Ofcom, 2012b. UK adults less concerned over internet despite privacy risks. *Ofcom.org*, Accessed from: <http://consumers.ofcom.org.uk/2012/03/uk-adults-less-concerned-over-internet-despite-privacy-risks/?lang=en> [Accessed June 18, 2012]

Office for National Statistics, 2011. Statistical bulletin: internet access – households and individuals. 2011, *Office for National Statistics*, 31 August

Oliveira, M., 2012. Canada's 'most socially networked' title slipping away. *The Globe and Mail*, [online]29 February, Accessed from: <http://www.theglobeandmail.com/technology/digital-culture/social-web/canadas-most-socially-networked-title-slipping-away/article550205/> [Accessed June 18, 2012]

Oliver, P., 2006. *The Sage Dictionary of Social Research Methods*. Jupp, V. ed., London: Sage Publications.

Olivero, N. and Lunt, P. Privacy versus willingness to disclose in e-commerce exchanges: the effect of risk awareness on the relative role of trust and control. *Journal of Economic Psychology* 25, pp.243–262.

Ostrow, A., 2007. Copycats: Top 10 international Facebook clones. *Mashable.com*, [online]11 July, Accessed from: <http://mashable.com/2007/07/11/10-facebook-clones/> [Accessed June 19, 2012]

Oxford Dictionaries, 2012. *Oxforddictionaries.com*, [online] Accessed from: <http://oxforddictionaries.com/definition/social%2Bnetwork> [Accessed May 15, 2012]

Paldam, M., 2000. Social capital: one or many? Definition and measurement. *Journal of Economic Surveys,*14(5), pp.629-653.

Palmer, A., and Koenig-Lewis, N., 2009. An experiential, social and network-based approach to direct marketing. *Direct Marketing: An International Journal*, 3(3), pp.162-176.

Pan, Y., and Zinkhan, G. M., 2006. Exploring the impact of online privacy disclosures on consumer trust. *Journal of Retailing*, 82(4), pp.331-338.

Parent, W. A., 1983. Privacy, morality, and the law. *Philosophy and Public Affairs*, 12(4), pp.269-288.

Parent, W. A., 1983. Recent work on the concept of privacy. *American Philosophical Quarterly*, 20, pp.341-355

Park, C. and Lessig, V.P., 1981. Familiarity and its impact on consumer decision biases and heuristics. *Journal of Consumer Research,* 8 (September), pp.223-230.

Park, C.W., Mothersbaugh, D.L., and Feick, L., 1994. Consumer knowledge assessment. *Journal of Consumer Research*, 21(June), pp.71-82.

Paxton, P., 1999. Is social capital declining in the United States? A multiple indicator assessment. *American Journal of Sociology*, 105(1), pp.88-127.

Petronio, S. S., 2002. *Boundaries of privacy: dialectics of disclosure*. Albany: State University of New York Press.

Pfeil, U., Arjan, R., and Zaphiris, P., 2009. Age differences in online social networking – a study of user profiles and the social capital divide among teenagers and older users of MySpace. *Computers in Human Behavior*, 25, pp.643-654.

Phelps, J., D'Souza and Nowak, G.J., 2001. Antecedents and consequences of consumer privacy concerns: an empirical investigation. *Journal of Interactive Marketing*, 15(4), pp.2-17.

Phelps, J., Nowak, G.J. and Ferrell, E., 2000. Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy and Management*, 19(1), pp.27-41.

Pitta, D.A., Franzak, F., and Laric, M., 2003. Privacy and one-to-one marketing: resolving the conflict. *The Journal of Consumer Marketing*, 20(7), pp.616-628.

Poddar, A., Mosteller, J., and Scholder E. P., 2009. Consumers' rules of engagement in online information exchanges. *Journal of Consumer Affairs*, 43(3), pp.419-448.

Portes, A., 1998. Social capital: its origins and applications in modern sociology. *Annual Review of Sociology,* 24, pp. 1-24.

Preece, J. and Maloney-Krichmar, D., 2005. Online communities: design, theory and practice. *Journal of Computer Mediated Communication*, 10(4):00.
DOI: 10.1111/j.1083-6101.2005.tb00264.x

Prosser, W. L., 1960. Privacy. *California Law Review*, 48(3), pp.383-423

PRWeb, 2011. Women are more dialed into social networks to communicate with work colleagues, friends, family, according to new survey from Rebtel. *PRWeb.com*, [online]22 September, Accessed from: <http://www.prweb.com/releases/prweb2011/9/prweb8819065.htm> [Accessed June 19, 2012]

Putnam, R.D., 1993. *Making democracy work: civic traditions in modern Italy*. Princeton, NJ: Princeton University Press.

Putnam, R.D., 1995a. Bowling alone: America's declining social capital. *Journal of Democracy*, January, pp.65-78.

Putnam, R.D., 1995b. Tuning in, tuning out: the strange disappearance of social capital in America. *PS: Political Science and Politics*, 28(4), pp. 664-683.

Putnam, R.D., 2000. *Bowling alone: the collapse and revival of American community*. New York: Simon and Schuster.

Putnam, R.D., 2001. Social capital: measurement and consequences. *Canadian Journal of Policy Research*, 2(1), pp. 41-51. Accessed May 14, 2013 from http://www.oecd.org/edu/country-studies/1825848.pdf

Rachels, J., 1975. Why privacy is important. *Philosophy and Public Affairs*, 4, pp.323-33.

Raice, S., 2011. Tagged acquires Facebook competitor Hi5. *The Wall Street Journal*. [online]14 December, Accessed from: <http://blogs.wsj.com/digits/2011/12/14/tagged-acquires-facebook-competitor-hi5/> [Accessed May 8, 2012]

Raju, P.S., Lonial, S.C., and Mangold, W.G., 1995. Differential effects of subjective knowledge, objective knowledge and usage experience on decision making: an exploratory investigation. *Journal of Consumer Psychology*, 4(2), pp.153-180.

Rapleaf, 2008. Rapleaf study of social network users vs. age. [online]18 June, Accessed from: <https://filesworkface.s3.amazonaws.com/bf161e8907f9a079e0270230df68d594/Rapleaf-Study-of-Social-Network-Users-vs-Age.pdf > [Accessed May 8, 2012]

Resnick, P., 2002. Beyond bowling together: sociotechnical capital. In J. Carroll (Ed.), *HCI in the New Millenium*, Boston, MA: Addison-Wesley. pp.247-272

Rheingold, H., 1993. *The virtual community: homesteading on the electronic frontier*. Reading, MA: Addison-Wesley Publishing.

Rifon, N. J., LaRose, R. J., and Lewis, M. L., 2007. Resolving the privacy paradox: toward a social-cognitive theory of consumer privacy protection. *Mimeo, Michigan State University*, Accessed from: <https://www.msu.edu/~wirthch1/privacyparadox07.pdf.>

Ringle, C.M., Wende, S., Will, A., 2005. SmartPLS 2.0. *SmartPLS Hamburg*, Germany, www.smartpls.de

Rose, E.A., 2005. An examination of the concern for information privacy in the New Zealand regulatory context. *Information and Management*, 43, pp.322-335.

Ruggerio, T.E., 2000. Uses and gratifications theory in the 21st century. *Mass Communication and Society*, 3(1), pp.3-37.

Saint Louis, C., 2011. Cellphones test the strength of gym rules. *The New York Times*. [online] Accessed from http://www.nytimes.com/2011/12/08/fashion/struggle-to-ban-smartphone-usage-in-gyms.html?pagewanted=all&_r=0. [Accessed July 28, 2013]

Sandefur, R., and Laumann, E., 1998. A paradigm for social capital. *Rationality and Society*, 10(4), pp. 481-501.

Sayre, S., and Horne, D. A., 2000. Trading secrets for savings: how concerned are consumers about club cards as a privacy threat? *Advances in Consumer Research*, 27, pp.151-155

Shah, S. K. and Corley, K. G., 2006. Building better theory by bridging the quantitative-qualitative divide. *Journal of Management Studies*, 43(8), pp.1821-35.

Scheufele, D.A. and Shah, D.V., 2000. Personality strength and social capital: the role of dispositional and informational variables in the production of civic participation. *Communication Research*, 27(2), pp. 107-131.

Schoeman, F. D.(ed.). 1984. *Philosophical Dimensions of Privacy: An Anthology*, Cambridge UK: Cambridge University Press

Schoenbachler, D.d. and Gordon, G.L., 2002. Trust and consumer willingness to provide information in database-driven relationship marketing. J*ournal of Interactive Marketing*, 16(3), pp.2-16.

Sheehan, K.B., 1999. An investigation of gender differences in on-line privacy concerns and resultant behaviors. *Journal of Interactive Marketing*, 13(4), pp.24-38.

Sheehan, K.B. and Hoy, M.G., 1999. Flaming, complaining and abstaining: How online users respond to privacy concerns. *Journal of Advertising*, 28(3), pp.37-51.

Sheehan, K.B. and Hoy, M.G., 2000. Dimensions of privacy concern among online consumers. *Journal of Public Policy and Marketing*, 19(1), pp.62-73.

Schneier, B., 2011. The eternal value of privacy. *Wired.com*, [online]18 May 2006, Accessed from: <http://www.wired.com/politics/security/commentary/securitymatters/2006/05/70886> [Accessed October 30, 2012]

Schwartz, B., 1968. The social psychology of privacy. *American Journal of Sociology*, 73 (May), pp. pp.741-752.

Science Encyclopedia, 2012. Privacy – definitions. [online], Accessed from: <http://science.jrank.org/pages/10852/Privacy-DEFINITIONS.html.> [Accessed August 21, 2012]

Singer, N., 2012. When a palm reader knows more than your life line. *The New York Times*. [online] Accessed from http://www.nytimes.com/2012/11/11/technology/biometric-data-gathering-sets-off-a-privacy-debate.html?_r=0. [Accessed July 28, 2013 from]

Sirdeshmukh, D., Singh, J. and Sabol, B., 2002. Consumer trust, value and loyalty in relational exchanges. *Journal of Marketing*, 66, pp.15-37.

Smith, A., 2011. Twitter Update 2011. *Pew Internet and American Life Project*, [online], Accessed from: <http://pewinternet.org/Reports/2011/Twitter-Update-2011/Main-Report.aspx> [Accessed May 8, 2012]

Smith, C., 2013. 17 Amazing Facebook stats. *Extended Ramblings*, [online]13 April, Accessed from: <http://expandedramblings.com/index.php/by-the-numbers-17-amazing-facebook-stats/0> [Accessed April 14, 2013]

Smith, H. J., Dinev, T. and Xu, H., 2011. Information privacy research: an interdisciplinary review. *MIS Quarterly*, 35(4), pp.989-1015.

Smith, H.J., Milberg, S.J., and Burke, S.J., 1996. Information privacy: measuring individuals' concerns about organizational practices, *MIS Quarterly*, 20 (2), 1996, pp.167-196.

Smith, J. B. and Barclay, D. W., 1997. The effects of organizational differences and trust on the effectiveness of selling partner relationships. *Journal of Marketing*, 61, pp.3-21.

Smith, J. K. and Heshusius, L., 1986. Closing down the conversation: the end of the quantitative-qualitative debate among educational enquirers. *Educational Researcher*,12, pp. 6-13.

Solove, D., 2006. A taxonomy of privacy. *University of Pennsylvania Law Review*, [online] 154(3), p. 477, Accessed from: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=667622> [Accessed August 1, 2011]

Spreng, R. A., Divine, R.L., and Page, T., 2001. An empirical examination of the differential effects of objective and subjective knowledge on information processing. *American Marketing Association Conference Proceedings*, 12, pp.329-335.

Stahl, B.C., 2004. Responsibility for information assurance and privacy: a problem of individual ethics? *Journal of Organizational and End User Computing*, 16(3), pp.59-78.

Statistics Canada, 2010. Statistics Canada CANSIM Table 358-0128. May 10, 2010, [Accessed September 7, 2011]

Steinfield, C., Ellison, N.B., and Lampe, C., 2008. Social capital, self-esteem, and use of online social network sites: a longitudinal analysis. *Journal of Applied Developmental Psychology*, 29, pp.434-445.

Stewart, D.W. and Shamdasani, P.N., 1990. *Focus groups: theory and practice*. London: Sage.

Stewart, K.A. and Segars, A.H., 2002. An empirical examination of the concern for information privacy instrument. *Information Systems Research*, 13(1), pp.36-49.

Stone, E.F., Gueutal, H.G., Gardner, D.G. and McClure, S., 1983. A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *Journal of Applied Psychology*, 68 (3), pp.459-468.

Strano, M. M., 2008. User descriptions and interpretations of self-presentation through Facebook profile images. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace,* [online] 2(2), article 1. Accessed from: <http://cyberpsychology.eu/view.php?cisloclanku=2008110402andarticle=1> [Accessed June 21, 2012]

Stroud, 2008. Social networking: An age-neutral commodity -- social networking becomes a mature web application. *Journal of Direct, Data and Digital Marketing Practice,* 9(3), pp.278-292

Stutzman, F., 2006. An evaluation of identity-sharing behavior in social network communities. *International Digital and Media Arts Journal*, 3(1), pp.10–18.

Stutzman, F., Vitak, J., Ellison, N. B., Gray, R., and Lampe, C., 2012. Privacy in interaction: exploring disclosure and social capital in Facebook. *In International Conference on Weblogs and Social Media (ICWSM'12*), Dublin, IE.

Subrahmanyam, K., Reich, S.M., Waechter, N., and Espinoza, G., 2008. Online and offline social networks: use of social networking sites by emerging adults. *Journal of Applied Developmental Psychology*, 29, pp.420-433.

Sujan, M., 1985. Consumer knowledge: effects on evaluation strategies mediating consumer judgments. *Journal of Consumer Research*, 12(June), pp.31-46.

Sullivan, M., 2011. 9 Reasons to switch from Facebook to Google+. *PCWorld*, [online]30 June Accessed from: <http://www.pcworld.com/article/234825/9_reasons_to_switch_from_facebook_to_google.html> [Accessed June 21, 2012]

Tax, S. S., Brown, S. W., and Chandrashekaren, M., 1998. Customer evaluations of service complaint experiences: implications for relationship marketing. *Journal of Marketing*, 62(2), pp.60-76.

Taylor, H., 2003. Most people are “privacy pragmatists” who, while concerned about privacy, will sometimes trade it off for other benefits. *Harris Interactive, The Harris Poll® #17*, [online], Accessed from: http://www.harrisinteractive.com/vault/Harris-Interactive-Poll-Research-Most-People-Are-Privacy-Pragmatists-Who-While-Conc-2003-03.pdf> [Accessed February 26, 2013]

Teddlie, C., and Tashakkori, A., 2009. *Foundations of mixed methods research: integrating quantitative and qualitative approaches in the social and behavioral sciences.* Thousand Oaks, CA: Sage.

Tenenhaus, M., 2008. Component-based structural equation modeling. *Total Quality Management & Business Excellence,* 19 (7–8), 871–886.

The Canadian Press, 2011. Ontario Privacy Commissioner warns Of smartphone data privacy issues, *The Huffington Post.* [online] Accessed from http://www.huffingtonpost.ca/2011/06/19/ontario-privacy-warning-smartphone-data_n_879940.html. [Accessed July 28, 2013]

Thornhill, T., 2011. Google Plus 'will have more than 400m users by the end of 2012' - will it overtake Facebook? *Daily Mail*, [online]30 December, Accessed from:

<http://www.dailymail.co.uk/sciencetech/article-2080207/Google-Plus-hit-400m-users--overtake-Facebook.html> [Accessed June 19, 2012]

Toriumi, F., Okada, I., Yamamoto, Y., Suwa, H., Izumi, K. and Hashimoto, Y., 2011. Classification of social network sites based on network indexes and communication patterns. *Proceedings of International Workshop on Social Web Mining Co-located with IJCAI2011 (2011(7)),* Accessed from: <http://hitoshi.isslab.org/study_work/2011/swm.pdf> [Accessed May 16, 2012]

Tow, W. N. F. H., Dell, P., and Venable, J. (2010). Understanding information disclosure behaviour in Australian Facebook users. *Journal of Information Technology*, 25(2), 126-136.

Tseng, G. (2011) Tagged acquires social network application Digsby. *Tagged.com*, Accessed May 8, 2012 from: http://about.tagged.com/biz-at-tagged/tagged-acquires-social-network-application-digsby-2/

Tuomela, R., 1995. *The importance of us: A philosophy study of basic social notions*. Stanford, CA: Stanford University Press.

Turow, J. Feldman, L. and Meltzer, K., 2005. Open to exploitation: American shoppers online and offline. *Annenberg Public Policy Center of the University of Pennsylvania*, [online]1 June, Accessed from: http://www.annenbergpublicpolicycenter.org/NewsDetails.aspx?myId=31. [Accessed May 23, 2012]

Turow, J., Hennessy, M. and Bleakley, A., 2008. Consumers' understanding of privacy rules in the marketplace. *Journal of Consumer Affairs*, 42(3), pp.411-424

Unknown, 2009. Top 25 social networking sites. [online] January, Accessed from: http://social-media-optimization.com/2009/02/top-twenty-five-social-networking-sites-feb-2009/] [Accessed August 25, 2011]

Utz, S., and Kramer, N., 2009. The privacy paradox on social network sites revisited: the role of individual characteristics and group norms. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace,* [online] 3(2), article 1, Accessed from: http://cyberpsychology.eu/view.php?cisloclanku=2009111001andarticle=1

Valenzuela, S., Park, N. and Kee, K.F., 2009. Is there social capital in a social network site?: Facebook use and college students' life satisfaction, trust and participation. *Journal of Computer-Mediated Communication*, 14, pp.875-901.

Van Dyke, T.P., Midha, V. and Nemati, H., 2007. The effect of consumer privacy empowerment on trust and privacy concerns in e-commerce. *Electronic Markets*, 17(1), pp.68-81.

Van Slyke, C., Shim, J.T., Johnson, R., and Jiang, J., 2006. Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems,* 7(6), pp.415-444.

Vasalou, A., Gill, A. J., Mazanderani, F., Papoutsi, C. and Joinson, A., 2011. Privacy dictionary: a new resource for the automated content analysis of privacy. *Journal of the American Society for Information Science and Technology,* 62 (11), pp. 2095-2105.

Ward, S., Bridges, K., Chitty, B., 2005. Do incentives matter? An examination of on-line privacy concerns and willingness to provide personal and financial information. *Journal of Marketing Communications*,11(1), pp.21–40.

Warren, S. D. and Brandeis, L. D., 1890. The right to privacy. *Harvard Law Review*, [online] IV(5), Accessed from: <http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html> [Accessed August 18, 2011]

Wasko, M.M. and Faraj, S., 2005. Why should I share? Examining social capital and knowledge contribution in electronic networks of practice. *MIS Quarterly*, 29(1), pp. 35 – 57.

Waters, S. and Ackerman, J., 2011. Exploring privacy management on Facebook: motivations and perceived consequences of voluntary disclosure. *Journal of Computer-Mediated Communication,* 17(2011), pp.101–115.

Wellman, B., 2001. Computer networks as social networks. *Science,* New Series, 293(5537) pp.2031-2034.

Wellman, B. and Frank, K., 2001. Network capital in a multilevel world: getting support from personal communities. In Lin, N., Cook, K., and Burt, R. (Ed.). *Social Capital: Theory and Research.* NY: Aldine DE Gruyter.

Wellman, B., Haase, A.Q., Witte, J. and Hampton, K., 2001. Does the internet increase, decrease, or supplement social capital? Social networks, participation, and community commitment. *American Behavioral Scientist*, 45(3), pp. 436-455.

Westin, A. F., 1967. *Privacy and freedom*. New York: Atheneum

Westin, A., 2003. Social and political dimensions of privacy. *Journal of Social Issues*, [online] 59(2), Accessed from: <http://www.privacysummersymposium.com/reading/westin.pdf> [Accessed July 30, 2011]

White, T.B., 2004. Consumer disclosure and disclosure avoidance. *Journal of Consumer Psychology* 14(1and2), pp.41-51

Whitley, E.A., 2009. Informational privacy, consent and the “control” of personal data. *EnCoRe: Ensuring Consent and Revocation*, [online], Accessed from: <http://www.encore-project.info/other_publications_material/EnCoRe%20Publication%20Privacy%20and%20Control.pdf> [Accessed April 12, 2013]

Wikipedia(a), 2012. Social network. Accessed from: <http://en.wikipedia.org/wiki/Social_network#cite_note-12> [Accessed May 15, 2012]

Wikipedia(b), 2012. List of social networking websites. Accessed from: <http://en.wikipedia.org/wiki/List_of_social_networking_websites> [Accessed May 8, 2012]

Williams, D., 2006. On and off the ‘net: scales for social capital in an online era. *Journal of Computer-Mediated Communication*, 11, pp.593-628.

Wimmer, R. D. and Dominick, J. R., 1994. *Mass media research: an introduction.* Belmont, CA: Wadsworth.

Winkler, S., 2001. Privacy: a modern challenge. *City of Cambridge, MA Consumer’s Council*, Accessed from: <http://www.ci.cambridge.ma.us/consumer/Privacy1.html> [Accessed June 14, 2011]

Wirtz, J., Lwin, M.O., and Williams, J.D., 2007. Causes and consequences of consumer online information privacy concern. *International Journal of Service Industry and Management*, 18(4), pp.326-348.

Wold, H., 1982. Systems under indirect observation using PLS. In: C. Fornell (Ed.). *A second generation of multivariate analysis. volume 1: Methods* (1st ed). New York, NY: Praeger. pp.325-347

Wolff, B., Knodel, J. and Sittitrai, W., 1993. Focus groups and surveys as complementary research methods. In: *Successful Focus Groups.* D.L. Morgan (ed.) London: Sage.

Woolcock, M., 1998. Social capital and economic development: toward a theoretical synthesis and policy framework. *Theory and Society*, 27, pp.151-208.

Xu, H., Dinev, T., Smith, H.J., and Hart, P., 2008. Examining the formation of individual's privacy concerns: toward an integrative view. In: *Proceedings of the 29th International Conference on Information Systems (ICIS)*, Paris, 1-16.

Xu, H., Dinev, T. Smith, H.J. Hart, P., 2011. Information privacy concerns: linking individual perception with institutional privacy assurances. *Journal of the Association of Information Systems*, 12(12), pp.798-824.

Yang, S. and Wang, K., 2009. The influence of information sensitivity compensation on privacy concern and behavioural intention. *The DATA BASE for Advances in Information Systems*, 40(1), pp.38-51

Youn, S., 2009. Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *The Journal of Consumer Affairs*, 43(3), pp.389-418.

Young, K., 2009. Online social networking: an Australian perspective. *International Journal of Emerging Technologies and Society*, 7(1), pp. 39-57

Young, K., 2011. Social ties, social networks and the Facebook experience. *International Journal of Emerging Technologies and Society*, 9(1), pp.20-34.

Zeithaml, V. A., 1981. How consumer evaluation processes differ between goods and services. *Marketing of services*, 9(1), pp.25-32.

Zhao, S., Grasmuck, S., and Martin, J., 2008. Identity construction on Facebook: digital empowerment in anchored relationships. *Computers in Human Behavior,* 24, pp. 1816-36.

Zucker, L.G., 1986. Production of trust: institutional sources of economic structure. 1840-1920*, Research in Organizational Behavior,* 8, pp. 53-111.

Appendix A

Appendix A.1 Objective Knowledge Items

Table A.1. Objective Knowledge Items Resulting from Original Privacy Quiz Created by the Office of the Privacy Commissioner of Canada

Survey Item	Original Question	Original Answer (Verbatim) http://www.priv.gc.ca/quiz/en/quiz.asp	Revised Question Answer Options = True, False, Don't Know	Correct Answer
OK 1	When obtaining consent, an organization can merely advise an individual of the purposes for which the information will be used. True False	False Principle 4.3, of PIPEDA states that the knowledge and consent of an individual are required for the collection, use, or disclosure of personal information, except where inappropriate. Principle 4.3.2 states that organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. It also requires that the purposes for the use or disclosure of personal information be clearly stated so that an individual can reasonably understand how the information will be used or disclosed. Therefore when obtaining consent, if an organization uses wording that is considered too broad - where it could be reasonable to conclude that the knowledge requirements under PIPEDA are not met - an organization could then be in contravention of PIPEDA. Please see the Privacy Commissioner of Canada's finding under PIPEDA Case Summary #2005-323 for additional information.	When obtaining consent from individuals, an organization can merely advise an individual of the purposes for which the information will be used.	**False**
OK 2	Consent to the collection, use or disclosure of personal information should not be a condition for supplying a product or a service, unless the information requested is required to fulfill an explicitly specified and legitimate purpose. True False	True Organizations should never make consent to collection, use or disclosure of personal information a condition for supplying a product or a service, unless the information requested is required to fulfill an explicitly specified and legitimate purpose. Please see the Privacy Commissioner of Canada's finding under PIPEDA Case Summary #2005-308 for additional reference.	Consent to the collection, use or disclosure of personal information should not be a condition for supplying a product or a service, unless the information requested is required to fulfill an explicitly specified and legitimate purpose.	**True**
OK 3	If there is legislated need to record an	False	If there is legislated need to record an	**False**

	identity document number, like a drivers licence number, the document should always be photocopied. True False	Many financial institutions record identification information, including driver's licence numbers in specific circumstances or for certain types of transactions. For example, the federal *Proceeds of Crime (Money Laundering) and Terrorist Financing Act and Regulations* explicitly require financial institutions to record identification numbers. This purpose has been found to be reasonable as it is legally necessary, and therefore in compliance with privacy legislation. However, very few organizations have legislated reasons for collecting driver's licence information. Even if it may be okay to record certain information, photocopying or scanning the licence generally goes too far. Why? The driver's licence contains more information than is needed for most business purposes, including a photograph, height and other physical descriptions, and signature. However, if according to law an organization is required to collect and keep a photocopy or copy of an identity document, then an organization must comply. For more information please see the Office of the Privacy Commissioner of Canada's Collection of Driver's Licence Numbers Under Private Sector Privacy Legislation.	identity document number, like a driver's license number, the document should always be photocopied.	
OK 4	The Personal Information Protection and Electronics Documents Act (PIPEDA) covers the: Collection, use or disclosure of personal information by federal government organizations. Collection, use or disclosure of personal information by organizations in the course of commercial activity. The collection, use or disclosure of personal information for journalistic, artistic or literary purposes.	Collection, use or disclosure of personal information by organizations in the course of commercial activity. PIPEDA sets ground rules for how organizations may collect, use or disclose information about individuals in the course of commercial activities. PIPEDA applies to organizations engaged in commercial activities across the country, except in provinces that have substantially similar private sector privacy laws. Quebec, Alberta and British Columbia each have their own law, and Ontario has a law which focuses specifically on personal health information that has been deemed substantially similar. Even in these provinces, PIPEDA continues to apply to the federally-regulated private sector and to personal information in inter-provincial and international transactions. PIPEDA also protects employee information, but only in the federally-regulated sector.	The Personal Information Protection and Electronics Documents Act (PIPEDA) covers the collection, use or disclosure of personal information by organizations in the course of commercial activity.	**True**

		For more information on PIPEDA please see the Office of the Privacy Commissioner of Canada's information sheet on Privacy Legislation in Canada and the Privacy Guide for Small Businesses.		
OK 5	An individual's Social Insurance Number should always be used to identify a customer. True False	False Privacy oversight agencies have long held the position that the Social Insurance Number (SIN) should not be used as a general identifier and that organizations should restrict the collection, use and disclosure of SINs to legislated purposes. Did you know that: ● Employers are authorized to collect SINs from employees in order to provide them with records of employment and T-4 slips for income tax and Canada Pension Plan (CPP) purposes. ● Organizations such as banks, credit unions, brokers and trust companies are required under the *Income Tax Act* to ask for customers' SINs for tax reporting purposes (e.g., interest earning accounts, RRSPs, etc.). ● No private-sector organization is legally authorized to request a SIN for purposes other than income reporting. Even for a financial institution, if a customer's account is not of a type that earns interest (e.g., if it is a credit account as opposed to a savings account), there is no legal requirement for the organization to collect the individual's SIN, and no obligation for the individual to supply it. The OPC recommends that no private sector organization request the SIN from a customer, and that no customer give the SIN to a private-sector organization, unless the organization is required by law to request it. For more information please see the Office of the Privacy Commissioner of Canada's Best Practices For The Use of Social Insurance Numbers in the Private Sector.	An individual's Social Insurance Number should always be used to identify a customer.	**False**
OK 6	An organization, which is subject to PIPEDA, uses overt video surveillance for justified security and crime prevention reasons but does not record any images. Since no images are recorded, compliance with PIPEDA is not an	False PIPEDA governs the collection, use and disclosure of information about an identifiable individual. In the private sector, surveillance through a video camera is subject to privacy laws. Under PIPEDA the information does not need to be recorded to constitute personal information. In addition to privacy legislation, organizations should ensure that the video surveillance complies	An organization, which is subject to PIPEDA, uses overt video surveillance for justified security and crime prevention reasons but does not record any images. Since no images are recorded, compliance with PIPEDA is not an	**False**

	issue. True False	with all applicable laws. For example, an organization using a video camera that captures sound may need to consider the *Criminal Code* provisions dealing with the collection of private communications. For more information please see the Office of the Privacy Commissioner of Canada's information sheet on Overt Video Surveillance in the Private Sector.	issue.	
OK 7	N/A	N/A	A privacy breach occurs when there is unauthorized access to, or collection, use, or disclosure of personal information.	**True**
OK 8	An individual can make a complaint to the Office of the Privacy Commissioner of Canada against an organization subject to PIPEDA: If they believe their personal information was improperly collected, used or disclosed. If an organization denies them access to their personal information. If an organization refuses to make changes to demonstrably inaccurate or incomplete information. If an organization refuses to record the substance of an unresolved challenge. All of the above.	All of the above. If an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization shall amend the information as required. In the case of an unresolved challenge, the substance of the unresolved challenge shall be recorded by the organization, however there is no obligation to change that information. For more information please see the Office of the Privacy Commissioner of Canada's Organizations' Guide to Complaint Investigations under the Personal Information Protection and Electronic Documents Act	An individual can make a complaint to the Office of the Privacy Commissioner of Canada against an organization subject to PIPEDA if an organization denies them access to their personal information.	**True**
OK 9	Under certain circumstances, an organization can disclose their customer’s personal information to law enforcement officials without their customer’s consent. True False	True Principle 4.5 of PIPEDA states that organizations should only disclose an individual's personal information when they have an individual's consent or when required by law. Section 7(3) of the *Personal Information Protection and Electronic Documents Act* states the limited instances where an organization can disclose an individual's personal information without	Under certain circumstances, an organization can disclose their customer’s personal information to law enforcement officials without their customer’s consent.	**True**

		their knowledge or consent. For example, disclosure without knowledge or consent can be made where required by law or if the disclosure is made to comply with a subpoena, warrant, order made by a court, or to comply with rules of court relating to the production of records. For more information please see the Office of the Privacy Commissioner of Canada's Guide for Businesses and Organizations - Exceptions to Consent on pg. 17.		
OK 10	When recording customer telephone calls, which one of these statements is false? Organizations may only record calls for specified purposes and the information collected must only be used for the specified purposes. Organizations must inform the individual that the call may be recorded but not the purposes for which the information will be used. The recording may only take place with the individual's consent. Organizations must ensure that they comply with the other provisions of PIPEDA with respect to matters such as safeguards, access, retention and disposal.	Organizations must inform the individual that the call may be recorded but not the purposes for which the information will be used. Conversations should not be recorded unless it is "for purposes that a reasonable person would consider are appropriate in the circumstances." The individual must be informed of the recording and the purposes and the call may only be recorded with the individual's consent, except in those very limited cases where consent is not required under PIPEDA. After being informed of the recording and its purposes, consent may generally be implied. For more information please see the Office of the Privacy Commissioner of Canada's information sheet on Guidelines for Recording of Customer Telephone Calls.	When recording customer telephone calls, organizations must inform the individual that the call may be recorded but not the purposes for which the information will be used.	**False**

Appendix A.2 Subjective Knowledge Items

Table A.2. Subjective Knowledge Items Resulting from Carlson et al's (2007) Scale of Subjective Knowledge of Pricing Tactics and Focus Group Feedback

Final Survey Item	**Original Survey Item**	**Original Question** **9 point Likert Scale**	**Modified Question Presented to Focus Group**	**Final Scale Items**
SK1	SK1	Please rate your knowledge of marketers' pricing tactics as compared to most people you know. 'One of the least knowledgeable' → 'One of the most knowledgeable'	Compared to most people you know, how would you rate your knowledge about how organizations collect and manage your personal information?	Compared to most people you know, how would you rate your knowledge about how organizations collect and manage your personal information?
SK2	SK2	In general, I am quite knowledgeable about marketers' pricing tactics. Strongly Agree' → 'Strongly Disagree'	In general, I am quite knowledgeable about how organizations collect and manage my personal information.	In general, I am quite knowledgeable about how organizations collect and manage my personal information.
--	SK3	I don't really know much about marketers' pricing tactics. Strongly Agree' → 'Strongly Disagree'	I don't really know much about how organizations collect and manage my personal information.	
SK3	SK4	I am knowledgeable of the different pricing tactics that marketers can use to make a product look attractive. Strongly Agree' → 'Strongly Disagree'	I am quite knowledgeable about how the information I provide in my online social network is collected and managed by companies.	I am quite knowledgeable about how the information I provide in my online social network is collected and managed by companies.
--	SK5	I have little knowledge regarding the pricing tactics that marketers use. Strongly Agree' → 'Strongly Disagree'	I don't really know much about how the information I provide in my online social network is collected and managed by companies.	

Appendix A.3 Concern for Information Privacy Items

Please indicate the extent to which you, as an individual, agree or disagree with each statement.

1=Strongly Disagree; 7=Strongly Agree

Think about the online social network you use most frequently and the company that provides the service (such as Facebook, Twitter or LinkedIn). Rate your level of agreement with each of the following statements.

Survey Item	**Question**	**Code***
CFIP1	It usually bothers me when companies ask me for personal information.	C1
CFIP2	All the personal information in computer databases should be double-checked for accuracy – no matter how much this costs.	E1
CFIP3	Companies should not use personal information for any purpose unless it has been authorized by the individuals who provided the information.	USU1
CFIP4	Companies should devote more time and effort to preventing unauthorized access to personal information.	IA1
CFIP5	When companies ask me for personal information, I sometimes think twice before providing it.	C2
CFIP6	Companies should take more steps to make sure that the personal information in their files is accurate.	E2
CFIP7	When people give personal information to a company for some reason, the company should never use the information for any other reason.	USU2
CFIP8	Companies should have better procedures to correct errors in personal information.	E3
CFIP9	Computer databases that contain personal information should be protected from unauthorized access – no matter how much it costs.	IA2
CFIP10	It bothers me to give personal information to so many companies	C3
CFIP11	Companies should never sell the personal information in their computer databases to other companies	USU3
CFIP12	Companies should devote more time and effort to verifying the accuracy of the personal information in their databases.	E4
CFIP13	Companies should never share personal information with other companies unless it has been authorized by the individuals who provided the information.	USU4
CFIP14	Companies should take more steps to make sure that unauthorized people cannot access personal information in their computers.	IA3
CFIP15	I'm concerned that companies are collecting too much personal information about me.	C4

*C=Collection; IA=Improper Access; USU=Unauthorized Secondary Use; E=Errors

Appendix A.4 Trust Items

Table A.4.1 Trust in Online Social Network Provider

Survey Item	**Original Scale Item**	**Final Scale Item**
	1=Strongly Disagree; 7=Strongly Agree	Think about the online social network you use most frequently and the company that provides the service (such as Facebook, Twitter, or LinkedIn). Rate your level of agreement with these statements. 1=Strongly Disagree; 7=Strongly Agree
	In general, FB…	**My online social network company...**
TP1	...is open and receptive to the needs of its members.	...is open and receptive to the needs of its members.
TP2	...makes good-faith efforts to address most members concerns.	...makes good-faith efforts to address most members concerns.
TP3	...is also interested in the well-being of its members, not just its own.	...is also interested in the well-being of its members, not just its own.
TP4	...is honest in its dealings with me.	...is honest in its dealings with me.
TP5	...keeps its commitments to its members.	...keeps its commitments to its members.
TP6	...is trustworthy.	...is trustworthy.

Table A.4.2. Trust in *ALL* Online Social Network Member Connections

Survey Item	**Original Scale Item**	**Final Scale Item**
	1=Strongly Disagree; 7=Strongly Agree	Think about the online social network you use most frequently and all the friends and connections you have there. Rate your level of agreement with these statements. 1=Strongly Disagree; 7=Strongly Agree
	Other members in the OSN…	**Generally speaking, all my friends and connections…**
TAM1	...will do their best to help me.	...will do their best to help me.
TAM2	...do care about the well-being of others.	...do care about the well-being of others.
TAM3	...are open and receptive to the needs of each other.	...are open and receptive to the needs of each other.
TAM4	...are honest in dealing with each other.	...are honest in dealing with each other.
TAM5	...keep their promises.	...keep their promises.
TAM6	...are trustworthy.	...are trustworthy.

Table A.4.3 Trust in *CLOSE* Online Social Network Member Connections

Survey Item	**Original Scale Item**	**Final Scale Item**
		Think about the online social network you use most frequently and only the friends and connections you share the most information with. Rate your level of agreement with these statements. 1=Strongly Disagree; 7=Strongly Agree
		The friends and connections that I share the most information with…
TCC1		...will do their best to help me.
TCC2		...do care about the well-being of others.
TCC3		...are open and receptive to the needs of each other.
TCC4		...are honest in dealing with each other.
TCC5		...keep their promises.
TCC6		...are trustworthy.

Appendix A.5 – Online Social Network Communication Privacy Management (OSN CPM) Items

Table A.5. Online Social Network Privacy Management Items Resulting from Child et al's (2009) Blogging Privacy Management Scale

	Actual Survey Question Number OSN PM	Code	Original Question	Modified Question	New Question
Boundary Ownership	1	BO1	I have limited the personal information posted on my blog.*	I have limited the personal information posted on my profile.*	
	4	BO2	I use shorthand (e.g., pseudonyms or limited details) when discussing sensitive information so others have limited access to know my personal information.*	I use shorthand (e.g., aliases or limited details) when discussing sensitive information so others have limited access to my personal information.*	
	7	BO3	If I think that information I posted really looks too private, I might delete it.*	If I think that information I posted really looks too private, I might delete it.*	
	10	BO4	I usually am slow to talk about recent events because people might talk.*	I am slow to talk about recent events because people might talk.*	
	13	BO5	I don't blog about certain topics because I worry who has access.*	I don't post about certain topics because I worry who can see it.*	
	16	BO6	Seeing intimate details about someone else, makes me feel I should keep their information private.*	Seeing intimate details about someone else makes me feel I should keep their information private.*	
	19	BO7			I never tag friends in photos.*
	22	BO8			When I am tagged in a photo I remove it immediately.*
	25	BO9			I do not share any of my contact information on my profile.*
	28	BO10			My birth date is not visible on my profile(s).*
	31	BO11			I would like to put my connections in groups so that different people can see different things.*
	34	BO12			I have changed my name to prevent people from finding me.*
Boundary Linkages	2	BL1	I have created a profile on my blog so that other bloggers can link to me with similar interests.	I have created a detailed profile so that others can link to me with similar interests.	
	5	BL2	I try to let people know my best interest on my blog so I can find friends.	I try to let people know my best activities and interests so I can find friends.	
	8	BL3	I allow people with a profile or picture I like to access my blog.	I allow people with a profile or picture I like to access my profile.	

	11	BL4	I comment on blogs to have others check out my blog.	I comment on or like things on friends’ pages to have others check out my profile.	
	14	BL5	I allow access of my blog through any of these: directories, key word searches, or weblog rings	I have my privacy settings set to ‘Everyone’.	
	17	BL6	I regularly link to interesting websites to increase traffic on my blog.	I like to link to interesting websites to increase traffic on my profile.	
	20	BL7			I use social networking links (like the Facebook ‘like’ button) on other websites.
	23	BL8			I support companies and people by ‘liking’ pages or making recommendations.
	26	BL9			I accept most friend or connection requests I receive.
	29	BL10			I like to add ‘applications’ to improve my experience.
	32	BL11			I feel uncomfortable saying no to ‘friend’ requests.
	35	BL12			I have a limited profile.
Boundary Permeability	3	BP1	When I face challenges in my life, I feel comfortable talking about them on my blog.	When I face challenges in my personal life, I feel comfortable talking about them.	
	6	BP2	I like my blog entries to be long and detailed.	I like my status updates or posts to be long and detailed.	
	9	BP3	I like to discuss work concerns on my blog.	I like to discuss work concerns publicly.	
	12	BP4	I often tell intimate, personal things on my blog without hesitation.	I often tell intimate, personal things without hesitation.	
	15	BP5	I share information with people whom I don’t know in my day-to-day life.	I share information with people whom I don’t know in my day-to-day life.	
	18	BP6	I update my blog frequently.	I update my profile frequently.	
	21	BP7		I update my status frequently.	
	24	BP8			When something positive happens to me, I post about it.
	27	BP9			My status updates generally indicate how I am feeling.
	30	BP10			I like to provide detailed comments on friends’ pages.
	33	BP11			When a friend in my network upsets me, I post about it.
	36	BP12			When a business upsets me, I post about it.

* Denotes the item has been reverse-scored

Appendix A.6 Survey Instrument

Online Social Network Attitudes

Thank you for volunteering to participate in this research. Your opinions about online social networks and your personal information are very important to us. Your answers will help researchers better understand how Canadians use online social networks and will contribute to building academic theory.

This research involves completing a questionnaire about your use of online social networks and opinions on related topics. It should take approximately 20 minutes of your time.The data collected will be used to complete a doctoral thesis at the University of Strathclyde in Glasgow, UK. Data is being collected solely for academic purposes and not for a corporate entity. The primary objectives of this research are to understand the ways in which individuals participate in online social networks and explore some influences that might affect decisions to participate.Ethics approval of the survey design and questionnaire has been granted by the University of Strathclyde. If you have any questions or concerns about this research, you may contact the researcher, Bobbi Morrison, at bmorriso@stfx.ca or else her supervisor {Prof. Alan Wilson, alan.wilson@strath.ac.uk}.Survey results will be aggregated for groups of respondents.

Your responses will be anonymous and confidential. No survey information collected will enable you to be personally identified in any way. All information is collected securely and data will be held in a password protected environment accessible by the researchers and will be destroyed after use.Your participation in this study is voluntary and you may stop taking the survey at any time. You have the right to refuse to participate now or at any point during the interview.Where an online survey is involved, we need to assure ourselves that the respondent is over 18 and is willing to participate in the study. We cannot accept under age respondents. By clicking on the link below you are agreeing that you are aged 18 or over, that you have read the description of the research objectives and you are willing to participate in this study.At the end of the survey you will be directed to a separate area to enter a prize draw. The contact details you provide will not be linked to your survey responses in any way.

Would you like to continue with the survey?

○ Yes

○ No

Here are a few introductory questions to get started. You must answer these three questions to proceed.

1. How old are you? Please select the appropriate age range below.

○ Under 18

○ 18 - 24

○ 25 - 34

○ 35 - 44

○ 45 - 54

○ 55 - 64

○ 65 or older

2. In which Canadian province or territory do you live permanently?

○ Alberta

○ British Columbia

○ Manitoba

○ New Brunswick

○ Newfoundland

○ Northwest Territory

○ Nova Scotia

○ Nunavut

○ Ontario

○ Prince Edward Island

○ Quebec

○ Saskatchewan

○ Yukon

○ None

3. Have you ever used an online social network such as Facebook, Twitter, Linked In, MySpace or Google+?

○ Yes

○ No

We are interested in the online social networking sites that you use and do not use.

1. From the list below, please identify which online social networks you currently use, no longer use, and have never used. Choose one option for each social network listed.

	Currently Use	No Longer Use	Have Never Used
Facebook	○	○	○
Twitter	○	○	○
MySpace	○	○	○
Linked In	○	○	○
Ning	○	○	○
Google+	○	○	○
Tagged	○	○	○
Classmates	○	○	○
hi5	○	○	○
Myyearbook	○	○	○
Meetup	○	○	○
Bebo	○	○	○

2. From this list, please indicate the social network you use most frequently.

Choose only one option.

○ Facebook

○ Twitter

○ MySpace

○ Linked In

○ Ning

○ Google+

○ Tagged

○ Classmates

○ hi5

○ Myyearbook

○ Meetup

○ Bebo

○ Other, please specify: ________________________

3. You identified that you visit {{OSN2}} most often. How frequently do you visit {{OSN2}}?Please choose the option that best indicates the number of times you visited {{OSN2}}last month.

LAST MONTH, I visited {{OSN2}}:

○ Not at all

○ One time

○ Two times

○ Once each week

○ A few times each week

○ Once each day

○ More than once per day

We are interested in learning about the ways you use online social networks.

Please indicate the extent to which each of the following statements is true or untrue by selecting the appropriate number below.

Think about {{OSN2}} and the ways you use it. Rate how true each of these statements is for you personally.1=Never True; 7=Always True

	Never True	2	3	4	5	6	Always True
1. I have limited the personal information posted on my profile.	○	○	○	○	○	○	○
2. I have created a detailed profile so that others can link to me with similar interests.	○	○	○	○	○	○	○
3. When I face challenges in my personal life, I feel comfortable talking about them.	○	○	○	○	○	○	○
4. I use shorthand (e.g., aliases or limited details) when discussing sensitive information so others have limited access to my personal information.	○	○	○	○	○	○	○
5. I try to let people know my best activities and interests so I can find friends.	○	○	○	○	○	○	○
6. I like my status updates or posts to be long and detailed.	○	○	○	○	○	○	○
7. If I think that information I posted really looks too private, I might delete it.	○	○	○	○	○	○	○
8. I allow people with a profile or picture I like to access my profile.	○	○	○	○	○	○	○
9. I like to discuss work concerns publicly.	○	○	○	○	○	○	○
10. I am slow to talk about recent events because people might talk.	○	○	○	○	○	○	○
11. I comment on or like things on friends' pages to have others check out my profile.	○	○	○	○	○	○	○
12. I often tell intimate, personal things without hesitation.	○	○	○	○	○	○	○

Continue thinking about {{OSN2}} and the ways you use it. Rate how true each of these statements is for you personally.1=Never True; 7=Always True

	Never True	2	3	4	5	6	Always True
13. I don't post about certain topics because I worry who can see it.	○	○	○	○	○	○	○
14. I have my privacy settings set to 'Everyone'.	○	○	○	○	○	○	○
15. I share information with people whom I don't know in my day-to-day life.	○	○	○	○	○	○	○
16. Seeing intimate details about someone else makes me feel I should keep their information private.	○	○	○	○	○	○	○
17. I like to link to interesting websites to increase traffic on my profile.	○	○	○	○	○	○	○
18. I update my profile frequently.	○	○	○	○	○	○	○
19. I never tag friends in photos.	○	○	○	○	○	○	○
20. I use social networking links (like the Facebook 'like' button) on other websites.	○	○	○	○	○	○	○
21. I update my status frequently.	○	○	○	○	○	○	○
22. When I am tagged in a photo I remove it immediately.	○	○	○	○	○	○	○
23. I support companies and people by 'liking' pages or making recommendations.	○	○	○	○	○	○	○
24. When something positive happens to me, I post about it.	○	○	○	○	○	○	○

Again, please think about {{OSN2}} and the ways you use it. Rate how true each of these statements is for you personally.1=Never True; 7=Always True

	Never True	2	3	4	5	6	Always True
25. I do not share any of my contact information in my profile.	○	○	○	○	○	○	○
26. I accept most friend or connection requests I receive.	○	○	○	○	○	○	○
27. My status updates generally indicate how I am feeling.	○	○	○	○	○	○	○
28. My birth date is not visible on my profile.	○	○	○	○	○	○	○
29. I like to add 'applications' to improve my experience.	○	○	○	○	○	○	○
30. I like to provide detailed comments on friends' pages.	○	○	○	○	○	○	○
31. I like to put my connections in groups so that different people can see different things.	○	○	○	○	○	○	○
32. I feel uncomfortable saying no to 'friend' requests.	○	○	○	○	○	○	○
33. When a friend in my network upsets me, I post about it.	○	○	○	○	○	○	○
34. I have changed my name on my profile to prevent certain people from finding me.	○	○	○	○	○	○	○
35. I have a limited profile that only allows very close connections to see my detailed information.	○	○	○	○	○	○	○
36. When a business or company upsets me, I post about it.	○	○	○	○	○	○	○

Here are some statements concerning your beliefs about the online social networks you use and the friend connections you have.

Please indicate the extent to which you, as an individual, agree or disagree with each statement by selecting the appropriate number.

Think about {{OSN2}}, THE COMPANY. Rate your level of agreement with these statements. 1= 'Strongly Disagree'; 7='Strongly Agree

My online social network company...

	Strongly Disagree	2	3	4	5	6	Strongly Agree
1. ...is open and receptive to the needs of its members.	○	○	○	○	○	○	○
2. ...makes good-faith efforts to address most members' concerns.	○	○	○	○	○	○	○
3. ...is also interested in the well-being of its members, not just its own.	○	○	○	○	○	○	○
4. ...is honest in its dealings with me.	○	○	○	○	○	○	○
5. ...keeps its commitments to its members.	○	○	○	○	○	○	○
6. ...is trustworthy.	○	○	○	○	○	○	○

Think about all the friends and connections you have in {{OSN2}} . Rate your level of agreement with these statements.1= 'Strongly Disagree'; 7='Strongly Agree

Generally speaking, all my friends and connections...

	Strongly Disagree	2	3	4	5	6	Strongly Agree
1. ...will do their best to help me.	○	○	○	○	○	○	○
2. ...do care about the well-being of others.	○	○	○	○	○	○	○
3. ...are open and receptive to the needs of each other.	○	○	○	○	○	○	○
4. ...are honest in dealing with each other.	○	○	○	○	○	○	○
5. ...keep their promises.	○	○	○	○	○	○	○
6. ...are trustworthy.	○	○	○	○	○	○	○

Think about ONLY the friends and connections you share the most information with in {{OSN2}}. Rate your level of agreement with these statements.1= 'Strongly Disagree'; 7='Strongly Agree

The friends and connections I share the most information with...

	Strongly Disagree	2	3	4	5	6	Strongly Agree
1. ...will do their best to help me.	○	○	○	○	○	○	○
2. ...do care about the well-being of others.	○	○	○	○	○	○	○
3. ...are open and receptive to the needs of each other.	○	○	○	○	○	○	○
4. ...are honest in dealing with each other.	○	○	○	○	○	○	○
5. ...keep their promises.	○	○	○	○	○	○	○
6. ...are trustworthy.	○	○	○	○	○	○	○

We would like to know how you rate your knowledge about the ways organizations manage your personal information.

Please select the answer that best represents how you feel.

Think about how ALL organizations and businesses you know manage your personal information.

1. Compared to most people you know, how would you rate your knowledge about how organizations collect and manage your personal information?

○ One of the least knowledgeable

○ Below average knowledge

○ Slightly below average knowledge

○ Average knowledge

○ Slightly above average knowledge

○ Above average knowledge

○ One of the most knowledgeable

Please indicate the extent to which you, as an individual, agree or disagree with this statement.

1= 'Strongly Disagree'; 7='Strongly Agree'.

	Strongly Disagree	2	3	4	5	6	Strongly Agree
2. In general, I am quite knowledgeable about how organizations collect and manage my personal information.	○	○	○	○	○	○	○

Now, think about {{OSN2}}. Please indicate the extent to which you, as an individual, agree or disagree with this statement.

1= 'Strongly Disagree'; 7='Strongly Agree'.

	Strongly Disagree	2	3	4	5	6	Strongly Agree
3. I am quite knowledgeable about how the information I provide in my online social network is collected and managed by companies.	○	○	○	○	○	○	○

We are interested in learning how you feel about the things online social network companies do with your personal information. This section contains some statements about your feelings on this topic.

Please indicate the extent to which you, as an individual, agree or disagree with each statement.

When reading these statements, think about <u>{{OSN2}} and other companies you know that provide online social networking services.</u>Rate your level of agreement with each of the following statements.

1=Strongly Disagree; 7=Strongly Agree

	Strongly Disagree	2	3	4	5	6	Strongly Agree
1. It usually bothers me when companies ask me for personal information.	○	○	○	○	○	○	○
2. All the personal information in computer databases should be double-checked for accuracy – no matter how much this costs.	○	○	○	○	○	○	○
3. Companies should not use personal information for any purpose unless it has been authorized by the individuals who provided the information.	○	○	○	○	○	○	○
4. Companies should devote more time and effort to preventing unauthorized access to personal information.	○	○	○	○	○	○	○
5. When companies ask me for personal information, I sometimes think twice before providing it.	○	○	○	○	○	○	○
6. Companies should take more steps to make sure that the personal information in their files is accurate.	○	○	○	○	○	○	○
7. When people give personal information to a company for some reason, the company should never use the information for any other reason.	○	○	○	○	○	○	○
8. Companies should have better procedures to correct errors in personal information.	○	○	○	○	○	○	○
9. Computer databases that contain personal information should be protected from unauthorized access – no matter how much it costs.	○	○	○	○	○	○	○
10. It bothers me to give personal information to so many companies.	○	○	○	○	○	○	○

11. Companies should never sell the personal information in their computer databases to other companies.	○	○	○	○	○	○	○
12. Companies should devote more time and effort to verifying the accuracy of the personal information in their databases.	○	○	○	○	○	○	○
13. Companies should never share personal information with other companies unless it has been authorized by the individuals who provided the information.	○	○	○	○	○	○	○
14. Companies should take more steps to make sure that unauthorized people cannot access personal information in their computers.	○	○	○	○	○	○	○
15. I’m concerned that companies are collecting too much personal information about me.	○	○	○	○	○	○	○

This section contains questions about Canadian rules concerning personal information.

The Government of Canada has rules about the ways an organization can use the personal information it collects from customers. According to those rules, identify which of the following statements are true and which are false.

	True	False	Don't Know
1. To get your permission to capture your personal information, an organization only needs to tell you the purposes for which the information will be used.	○	○	○
2. Organizations can always refuse to supply a product or service if you won’t give permission to the collection, use or disclosure of your personal information.	○	○	○
3. If an organization is required by law to record an identity document number, like a driver’s license number, the document should always be photocopied by the organization.	○	○	○
4. Canada’s Personal Information Protection and Electronics Documents Act (PIPEDA) covers the collection, use or disclosure of personal information by organizations in the course of commercial activity.	○	○	○
5. All Canadian organizations can collect your Social Insurance Number so they can identify you.	○	○	○
6. An organization, which is subject to PIPEDA, uses overt video surveillance for justified security and crime prevention reasons but does not record any images. Since no images are recorded, compliance with PIPEDA is not an issue.	○	○	○
7. A privacy breach has occurred when there is unauthorized access to, or collection, use, or disclosure of personal information.	○	○	○
8. An individual can make a complaint to the Office of the Privacy Commissioner of Canada against an organization if an organization denies them access to their personal information.	○	○	○
9. Under certain circumstances, an organization can disclose their customer’s personal information to law enforcement officials without their customer’s consent.	○	○	○
10. When recording customer telephone calls, organizations must inform the individual that the call may be recorded but not the purposes for which the information will be used.	○	○	○

You are almost finished the survey. We just need to know a few more things about you.

Please indicate which of the following devices you use to connect to the Internet. <u>Check all that apply.</u>

□ Desktop computer

□ Laptop computer

□ Netbook

□ iPad/tablet

□ Cellphone

□ iPod/MP3 player

□ Game console

□ Portable gaming device

□ e-book reader

□ Other, please specify: _______________________

Please identify your gender.

○ Male

○ Female

○ Prefer not to answer

How would you describe where your home is located?

○ Urban area

○ Rural area

Please specify your mother tongue.

○ English

○ French

○ Other _______________________

How would you describe your race?

○ White / Caucasian

○ Black / African Canadian

○ Asian

○ Pacific Islander

○ Aboriginal

○ Indian

○ Spanish / Hispanic / Latino

○ Other _______________________

○ Prefer Not to Answer

Please identify the highest level of education you have completed.

○ Did not complete high school

○ High school or equivalent

○ College diploma

○ Bachelor's degree

○ Master's degree

○ Doctoral degree

○ Other, please specify: _______________________

○ Prefer not to answer

Please select the option that best represents your household income.

○ Under $20,000

○ $20,000 - $39,999

○ $40,000 - $59,999

○ $60,000 - $79,999

○ $80,000 - $99,999

○ $100,000 or more

○ Prefer Not to Answer

How did you hear about this survey?

○ Facebook ad

○ Linked In ad

○ Email

○ Referred by a friend

○ PIAC Newsletter

○ StFX Research Panel participant

○ Other