2022

Social Media Analytics and Information Privacy Decisions: Impact of User Intimate Knowledge and Co-ownership Perceptions

Bradley Alukwe Wangia
Nova Southeastern University, bradley.wangia@gmail.com

Social Media Analytics and Information Privacy Decisions: Impact of User Intimate Knowledge and Co-ownership Perceptions

by

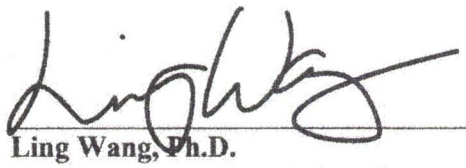
Bradley A. Wangia

A Dissertation Submitted in Fulfillment of the Requirements
for the Degree of Doctor of Philosophy
in
Information Systems

College of Computing and Engineering
Nova Southeastern University

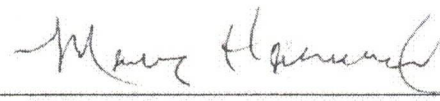
2022

We hereby certify that this dissertation, submitted by Bradley A. Wangia conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.



Ling Wang, Ph.D.
Chairperson of Dissertation Committee

6/16/22
Date



Mary Harward, Ph.D.
Dissertation Committee Member

6/16/22
Date

Junping Sun, Ph.D.
Dissertation Committee Member

6/16/22
Date

Approved:

Meline Kevorkian, Ed.D.
Dean, College of Computing and Engineering

6/16/22
Date

College of Computing and Engineering
Nova Southeastern University

2022

An Abstract of a Dissertation Submitted to Nova Southeastern University in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

Social Media Analytics and Information Privacy Decisions: Impact of User Intimate Knowledge and Co-ownership Perceptions

by
Bradley A. Wangia
June 2022

Social media analytics has been recognized as a distinct research field in the analytics subdomain that is developed by processing social media content to generate important business knowledge. Understanding the factors that influence privacy decisions around its use is important as it is often perceived to be opaque and mismanaged. Social media users have been reported to have low intimate knowledge and co-ownership perception of social media analytics and its information privacy decisions. This deficiency leads them to perceive privacy violations if firms make privacy decisions that conflict with their expectations. Such perceived privacy violations often lead to business disruptions caused by user rebellions, regulatory interventions, firm reputation damage, and other business continuity threats. Existing research had developed theoretical frameworks for multi-level information privacy management and called for empirical testing of which constructs would increase user self-efficacy in negotiating with firms for joint social media analytics decision making.

A response to this call was studied by measuring the constructs in the literature that lead to normative social media analytics and its information privacy decisions. The study model was developed by combining the relevant constructs from the theory of psychological ownership in organizations and the theory of multilevel information privacy. From psychological ownership theory, the impact that intimate knowledge had on co-ownership perception of social media analytics was added. From the theory of multi-level information privacy, the impact of co-ownership perception on the antecedents of information privacy decisions: the social identity assumed, and information privacy norms used were examined. In addition, the moderating role of the cost and benefits components of the privacy calculus on the relationship between information privacy norms and expected information privacy decisions was measured.

A quantitative research approach was used to measure these factors. A web-based survey was developed using survey items obtained from prior studies that measured these constructs with only minor wording changes made. A pilot-study of 34 participants was conducted to test and finalize the instrument. The survey was distributed to adult social media users in the United States of America on a crowdsourcing marketplace using a commercial online survey service. 372 responses were accepted and analyzed. The partial least squares structural equation modeling method was used to assess the model and analyze the data using the Smart partial least squares 3 statistical software package.

An increase in intimate knowledge of social media analytics led to higher co-ownership perception among social media users. Higher levels of co-ownership perception led to higher expectation of adoption of a salient social identity and higher expected information privacy norms. In addition, higher levels of expectation of social information privacy norm use led to normative privacy decisions. Higher levels of benefit estimation in the privacy calculus negatively moderated the relationship between social norms and privacy decision making. Co-ownership perception did not have a significant effect on the cost estimation in social media analytics privacy calculus. Similarly, the cost estimation in the privacy calculus did not have a significant effect on the relationship between information privacy norm adoption and the expectation of a normative information privacy decision.

The findings of the study are a notable information systems literature contribution in both theory and practice. The study is one of the few to further develop multilevel information privacy theory by adding the intimate knowledge construct. The study model is a contribution to literature since its one of first to combine and validate elements of psychological ownership in organization theory to the theory of multilevel information privacy in order to understand what social media users expect when social media analytics information privacy decisions are made. The study also contributes by suggesting approaches practitioners can use to collaboratively manage their social media analytics information privacy decisions which was previously perceived to be opaque and under examined. Practical suggestions social media firms could use to decrease negative user affectations and engender deeper information privacy collaboration with users as they seek benefit from social media analytics were offered.

Acknowledgements

I would like to thank all those who gave me guidance, support and encouragement as I worked to complete this dissertation. I owe them all a debt of gratitude. My sincere thanks to my dissertation chair Dr. Ling Wang. Her guidance truly enabled me to focus on every detail at each step of the process. I'm thankful for her guidance, feedback, and suggestions that helped me overcome the huddles I encountered along the way. I am sincerely grateful for Dr. Wang without whom I would not have completed the dissertation.

I would also like to thank my dissertation committee members Dr. Mary Harward and Dr. Junping Sun. Their encouragement validated my approach and suggestions challenged me and improved my dissertation immensely. Their feedback and recommended approaches were crucial in completing the dissertation. I would like to thank all the friends, family members, and professional network colleagues who participated in my pilot study. Without their feedback I would not have been able to improve the study instrument.

I also want to thank my family who gave me material, moral, and spiritual support. I would like to thank my late mother, Dr. Benigna Wangia. Watching her trust in God and work on her dissertation as a child taught me well and inspired me to complete my own. Her reliance on prayerful inquiry guided my own approach. Thank you to my father, Gideon, for his constant belief and encouragement. My gratitude for the support from my siblings Cynthia, Christian, Arlene, Hector, and Annette. A note of thanks to my extended family for all their encouragement and for their inquiries on when I would complete my doctorate. A big thank you to my wife Katherine without whom I would not have completed this dissertation. I would also like to thank my sons Joshua, Jacob, and Jonathan for their patience when I had to step away to work on the dissertation.

Table of Contents

List of Tables

Tables

List of Figures

Figures

Chapter 1

Introduction

Background

Social media (SM) users have been reported to have low knowledge of how companies use their data to generate analytics for business purposes (Acquisti et al., 2015; Hermes et al., 2020). Companies, on the other hand, acknowledged that SM users' data was key to creating social media analytics (SMA) even though users had been unaware how this type of analytics was created and used (Pole, 2010). SMA is used internally or disclosed externally to business partners for business critical purposes including to improve marketing strategy, increase customer engagement, enhance firm's reputation, improve hiring, detect fraud, and for many other important business functions (Holsapple et al., 2018). This use often leads to negative user affectations when a company's SMA privacy decisions are contrary to the privacy norms SM users expect. Counter-normative SMA use incidents have been reported where general health information had been revealed, unwanted pregnancy status disclosed, sexual orientation disclosed, elections influenced, among others (Barth-Jones, 2012; Bélanger & Crossler, 2019; Duhigg, 2012; Narayanan & Shmatikov, 2006).

A New York Times article on Target Inc.'s SMA use illustrated the problem and offered an example of this phenomenon (Duhigg, 2012). Duhigg (2012) reported that at a store in Minneapolis, an irate father confronted Target staff for promoting teen pregnancy to his daughter. The confrontation was a result of Target's analytics correctly predicting the girl's pregnancy. Based on SMA, the company had sent the girl coupons for baby

supplies at the address she shared with her father. Target Inc. unwittingly disclosed the girl's pregnancy status to her father before she chose to do so herself. From Pole's (2010) presentation prior to this incident at an analytics trade event, one learns that his employer, Target Inc, utilized SM data in developing its predictive analytics and Target did so with the aim of benefitting its customers. However, by Poole's (2010) admission, the company's SMA creation, use, and disclosure decisions did not include SM user intimate knowledge or co-ownership. Several questions then arise, would the girl have collaborated with Target and contributed to normative privacy rules that protected her information differently if she had intimate knowledge and co-ownership of Target's SMA creation? Would she have given input into the salient social identities used in the processes? Would she have prevented a privacy violating information privacy decision if she had co-ownership perceptions of the resulting SMA? The literature suggested that she would.

Problem Statement

Low social media analytics intimate knowledge and co-ownership perception (COP) among social media users lead to unexpected privacy decisions which result in business disruptions (Acquisti et al., 2015; Bélanger & James, 2020; Yun et al., 2019).

Bélanger and James (2020) in the theory of multilevel information privacy (TMIP) proposed that users would perceive privacy violations when companies make SMA privacy decisions using information privacy norms (IPN) that are not mutually agreed-upon. This makes sense since information privacy has been defined as the ability to control one's information in individual, group, organizational, and societal contexts (Bélanger & Crossler, 2011; Smith et al., 2011). In this definition, the word "one's"

points to the ownership perception that is key to claiming the right to control use or interaction by others. Psychological ownership (PO) in organizations theory pointed out that intimate knowledge of an object was a precursor to ownership perceptions (Pierce et al., 2001). Bélanger and James (2020) subsequently theorized in TMIP that ownership perception influenced the antecedents of multilevel information privacy decisions (MIPD). Bélanger and James (2020) also suggested that users perceive privacy violations when a company makes counter-normative MIPDs. In their view, such MIPDs were made due to lower weight ascribed to other co-owners' ownership claims and subsequently the salient social identity adopted, information privacy rules used or due to the influence of the cost-benefit estimation in the privacy calculus on the rules used to make the privacy decision. This study combined these two theories to contribute by empirically testing the effect of intimate knowledge on co-ownership perception which then affected the antecedents of information privacy decisions.

Existing empirical studies on SMA privacy management appeared to use models for privacy preservation in the analytics creation and distribution but not in its use for information privacy decisions. Protecting privacy in the creative steps of data preparation, data exploration, data analysis, and analysis publishing was the focus of much of the analytics privacy literature (Suseno et al., 2018; Tran & Hu, 2019). The privacy preserving methods used in the preparation, exploration and analysis phases included de-identification, cryptography, data perturbation, anonymity models, and differential privacy (Martens et al., 2016; Tran & Hu, 2019). The analytics publishing step preserved privacy by using various tooling and metrics to detect and report potential errors in the privacy preservation (Tran & Hu, 2019). Many of these approaches appeared

to assume that by obtaining SM user privacy consent to analyze, then removing personal identifiable information, the company gained sole ownership of the resulting analytics. This sole ownership perception appeared to lead firms to assume they did not need to familiarize SM users with the resulting SMA or involve them in the privacy decision making process.

Existing studies removed personal information to preserve information privacy in the content of SMA generation. These studies did not sufficiently explore this study's identified problem of which user constructs were relevant for effective multilevel SMA privacy decision making and how users become motivated to affect privacy decisions. This study examined the role of SM users as key contributors to the social identity assumed for a privacy decision, contributors to mutually agreed-upon SMA information privacy norms, and the influence of the evaluation of the cost and benefits components of the privacy calculus once they have intimate knowledge of and co-ownership of SMA.

SM user's data disclosures had previously been reported to be integral to creation of SMA (Holsapple et al., 2018) and so SM users should have maintained ownership rights and become part of SMA privacy decision making. Bélanger and James (2020) in TMIP suggested that where an entity was integral to the creation of information, that entity should be accorded ownership rights and should negotiate privacy rules with the organization holding the co-created information. A review of the literature reveals little evidence of such negotiations for SMA. There was some empirical research examining co-ownership in social media (Zhu & Kanjanamekanant, 2020) but the study restricts itself to raw SM data and its use and not SMA. Examining SMA privacy management was important because unlike SM data which was typically known and disclosed by SM

users, SMA tends to be more hidden from SM user view since it was generated after the fact and because organizations held it as a proprietary asset for competitive advantage use often out of common view (Holsapple et al., 2018). Zhu and Kanjanamekanant's (2020) study showed that SM data co-ownership perception was positively correlated with perceived privacy, moderates the positive relationship between negative affectations and the use of SM internal data, and moderates the negative relationship between ad embarrassment and perceived privacy in advertising context (Zhu & Kanjanamekanant, 2020). In Zhu and Kanjanamekanant's (2020) study, co-ownership was examined but the focus was SM data use which unlike SMA, was typically intimately known to the SM user. The poorly understood influence of SM users' low intimate knowledge and co-ownership perception of SMA and resulting privacy violations threatens to disrupt SMA business use via user rebellions, government regulatory interventions, and company reputation damage (Acquisti et al., 2015; Sweeney, 2002; Tanner, 2016). These negative affectations threaten to remove the large societal benefits that many downstream businesses offer from SMA.

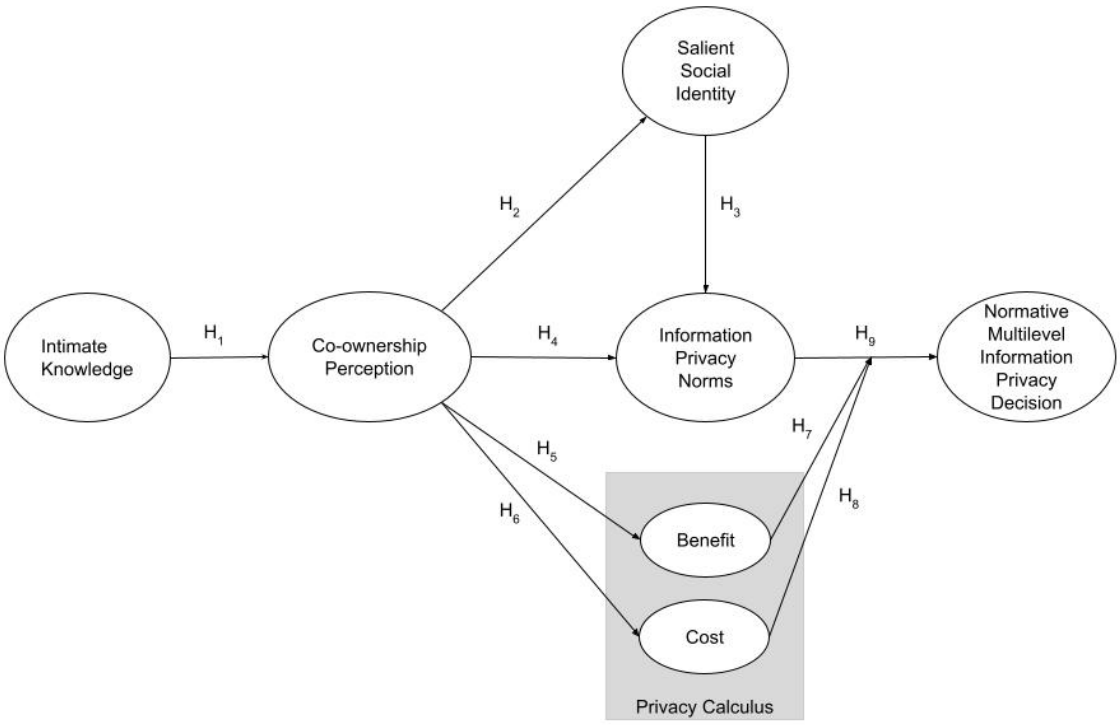
Dissertation Goal

The goal of this study was to examine the influence of various constructs on social media analytics information privacy management. First, the impact of intimate knowledge of SMA had on its co-ownership perception was examined. Second, the influence of co-ownership perception on the expected social identity used to make the privacy decision was evaluated. Third, the impact of the adopted social identity on the information privacy norm was examined. Fourth, the impact of co-ownership perception on the information privacy norm used in privacy decision making was measured. Fifth

and sixth, the impact of the co-ownership perception on the cost-benefit estimation of the privacy calculus on the relationship between information privacy norms and SMA privacy decision making was explored. Seventh and eighth, the moderating effects of the cost and benefit estimations of the privacy calculus on the relationship between information privacy norm use and the SMA privacy decision made was explored. Finally, the impact of the adopted social norm on the expected information privacy decision was examined. This study's proposed model is illustrated in Figure 1.

Figure 1

Research Model



The research model was developed by combining constructs from psychological ownership in organizations theory (Pierce et al., 2001) with the co-ownership influenced

constructs from the TMIP (Bélanger & James, 2020). Previous information privacy reviews had called for study using theoretical frameworks that allow for multiple levels of analysis beyond personal and to include combinations of individual, group, organization, and societal levels as well (Pavlou, 2011). Adapting constructs from the TMIP for building the model, this study answered Pavlou‘s (2011) call for studies to examine the combination of the individual and organizational information privacy contexts since SMA information privacy involves both the individual user and the organization. The psychology of ownership in organizations theory contributed the role that intimate knowledge construct plays on the development of co-ownership perception. The study next explored the theoretical underpinnings of the relationships between the constructs.

Research Hypotheses

Pierce et al. (2001) posited in the social sciences literature that organizational users develop ownership perceptions due to intimate knowledge of a target object. This ownership perception developed using three self-identity routes: controlling the target, knowing the target intimately, and investing self into the target. For SMA, the user did not control the target since SMA was typically in the company's custody. This study therefore focused on measuring intimate knowledge and investing of self. The effect of intimate knowledge on ownership perception while acknowledged in SM was not a guaranteed phenomenon and where and how it developed had been reported to be context specific (Kwon, 2020). Kwon (2020) showed that increased intimate knowledge in SM led to lower engagement and ownership due to loss of novelty. In another study, Pierce et al.’s (2001) PO theory was extended to develop a needs-affordances-features (NAF)

perspective on social media use (Karahanna et al., 2018). In NAF, Karahanna et al. (2018) showed that PO theory's self-identity constructs of SM users' psychological ownership applied in the social media context. They encouraged use of their NAF perspective to empirically test other constructs in psychological ownership theory in social media. This study is a response to this call in the SMA context and hypothesized that increased intimate knowledge of SMA would lead to increased co-ownership perception. Additionally, the TMIP holds that co-creators were already co-owners even if they don't know it yet (Bélanger & James, 2020). Therefore, it was hypothesized that an increase in intimate knowledge of how SMA was created from SM user disclosures and SM activity would increase SM users' SMA co-creator and co-owner perception. As such it was expected that higher SMA intimate knowledge by SM users would lead to higher SMA co-ownership perception.

H_1: SM users' intimate knowledge of SMA generated from their SM content is positively correlated to their SMA co-ownership perception.

Beliefs about whether enterprises or individuals own information had been shown to affect whether personal or group identity were adopted when making disclosure decisions (Constant et al., 1994; Jarvenpaa & Staples, 2001). Constant et al. (1994) demonstrated that the identity assumed for decisions depended on whether the user ascribed more weight to the role of their own personal attributes like expertise in information creation or whether they viewed the information more as a product of the organization's processes. Users have been shown to recognize an enterprise's legitimate but limited right to control and use their information when they negotiate use with the enterprise and assume joint social identities with firms (Gabisch & Milne, 2014; Sharma & Crossler, 2014). The

individual and the organization acted as distinct entities or as a group in these information privacy disclosure actions. User and organization joint participation in a group in the literature was illustrated in the case of brand communities where the users and the organization jointly formed a group with a social identity distinct from the user or the enterprise (Algesheimer et al., 2005). Additionally, privacy decisions making social units had been shown to either be group or individually aligned and used privacy rules specific to the social unit adopted (Hong & Thong, 2013; Laufer & Wolfe, 1977). Earlier studies had shown that the more a user perceived themselves as a member of a group the less the salience of their personal identity and the greater the group's social identity (Bergami & Bagozzi, 2000). Therefore, it was hypothesized that the higher SM users' SMA co-ownership perception with the SM company was, the more likely they were to assume a group social identity.

H_2: Perception of SMA co-ownership is positively correlated with a salient social identity.

The social sciences literature held that individuals had a self-concept that draws from the extent of knowing and identifying with group membership (Tajfel, 1974). Users who identified and self-categorized themselves into a group membership adopted citizenship behaviors for that group rather than their personal norms (Bergami & Bagozzi, 2000). IS studies demonstrated that personal or group self-concept affected users' levels of participation in virtual communities (Tsai & Bagozzi, 2014). Tsai and Bagozzi (2014) outlined that group and personal social identities map to corresponding group and personal social norm expectation respectively. Consequently, it was posited that the salient social identity adopted for SMA would influence SM users' expectation of which

social identity's information privacy norms would be applied to manage SMA privacy decisions.

H_3: SMA salient social identity is positively correlated with the level of expectation that information privacy norms (IPNs) for that identity was utilized.

Turner and Reynolds (2012) held in their development of self-categorization theory (SCT) that users perceived themselves as being both unique individuals and members of multiple groups and could move between these perceptions. Bélanger and James (2020) relied on SCT in developing TMIP to argue that the IPN, personal or group, the SM user expects to be used in the multilevel privacy decision was influenced by their levels of co-ownership perception in that group. Self-categorization theory outlined that while individuals had several social identities, they evaluated and adopted salient social identity based on environmental characteristics (Turner & Reynolds, 2012). One key environmental characteristic reported to be germane to privacy decision making was co-ownership perception (Bélanger & James, 2020). As such, it was expected that high levels of co-ownership perception in a particular group would positively correlate with the SM users' expectation of that same group's norms would be utilized in SMA privacy decision making.

H_4: SMA co-ownership perception in a particular group is positively correlated with the expectations of use of the same group's salient social identity's IPNs.

The TMIP theorizes that the level of ownership perception would influence the cost or benefit estimate of the privacy calculus during privacy decisions and called for empirical testing (Bélanger & James, 2020). In prior research, higher levels of personal ownership

perception had previously been shown to reduce the willingness to disclose personal information in social media specifically (Cichy et al., 2014) and in general IS contexts (Sharma & Crossler, 2014). However, relinquishing sole right to ownership of data had been shown to increase the propensity to disclose information (Gabisch & Milne, 2014). As such, it was hypothesized that higher levels of co-ownership perception would lead to higher levels of benefits estimation in the privacy calculus. It was also hypothesized that higher levels of co-ownership perception would lead to corresponding lower estimation of costs in the privacy calculus.

H_5: SMA co-ownership perception is positively correlated with the benefit estimation in the privacy calculus.

H_6: SMA co-ownership perception is negatively correlated with cost estimation in the privacy calculus.

The TMIP suggested that IPNs that were normative to the stimulated salient social identity would be used to make the privacy decision unless the cost was too high relative to the benefit (Bélanger & James, 2020). As such it was hypothesized that the user expected more normative MIPDs would be made when the more normative IPN was selected. The privacy calculus constructs had been shown in the social media context to estimate intention to make information privacy decisions (Krasnova & Veltri, 2010). As such this study expects that high costs in the privacy calculus moderate the positive relationship from normative IPNs to the normative privacy decision. Additionally, low benefits in the privacy calculus would moderate the positive relationship from normative IPNs to the normative privacy decision.

H_7: Benefits in the privacy calculus moderate the positive relationship of normative IPNs with normative MIPDs.

H_8: Costs in the privacy calculus moderate the positive relationship of normative IPNs with normative MIPDs.

H_9: Normative IPNs for the salient social identity are positively correlated with a normative privacy decision.

Relevance and Significance

Gaining understanding of the influence of user intimate knowledge and co-ownership perception on the antecedents of information privacy decisions was a relevant problem because it would give both firms and SM users empirical evidence in a previously poorly understood phenomenon relevant to SMA information privacy management practice. Leading firms had been reported to use SMA for a wide array of business-critical functions such as product development, pre-employment screening, fraud detection, marketing, personal health, competitor intelligence, and improving the public good (Bughin & Chui, 2010; Dong et al., 2018; Fan & Gordon, 2014; Hu et al., 2019; Montaquila & Godwin, 2016; Poom et al., 2020). Recent studies demonstrated even higher potential for super-additive business value for firms by integrating SMA from various channels into business processes (Dong & Yang, 2020). SMA information privacy violation perceptions pose a serious challenge to the ability for society to benefit from this super-additive business value.

Despite early warnings, information privacy violations had led to negative user affectations and government interventions against SM firms (Acquisti et al., 2015; Sweeney, 2002; Tanner, 2016). SMA theory and practice had produced service and

business gains, only to later contend with privacy concerns from social media (SM) users, regulators, and the general public (Holsapple et al., 2018; Zetter, 2009). This inadequate theory had forced firms to manage the negative effects of information privacy violations by defending themselves in court, testifying before legislatures, and running public relations programs (Hermes et al., 2020; Malhotra et al., 2004; Singel, 2009; White et al., 2008). Firms had attempted to change their privacy management practices and disclosures, but these efforts were often viewed as superficial (Bélanger & James, 2020). Bélanger and James (2020) referred to the example of Facebook's change in SMA information disclosure behavior after negative affectations from a counter-normative information privacy decision in the Cambridge Analytica scandal as a temporary method of assuaging public anger. They believed that firms such as Facebook were only likely to continue these short-term fixes for as long as public malcontent persisted. This leads one to ask whether the information systems (IS) literature has a more effective theoretical way to manage SMA information privacy? Could theory based empirical study help firms provide sufficient SMA information privacy management to satisfy SM users and business intentions alike?

Historically, information privacy research had lacked group studies, and practice had been reported to suffer accordingly (Bélanger & Crossler, 2011; Bélanger & Xu, 2015; Smith et al., 1996). This study contributed important group literature that impacts the wide segment of society that utilizes SMA. SM users had been reported to have low knowledge of the use of their SMA and low information ownership claims because they potentially did not know when their personal information was used in SMA creation (Chen et al., 2017; Pavlou et al., 2007). Having a clear understanding of the role of

intimate knowledge and co-ownership was likely to produce cognitive benefits that contribute to individual, firm, and societal well-being.

Barriers and Issues

A couple of barriers and an issue have existed in the literature when examining privacy implications of social media analytics business use. The first barrier to solving the identified problem was the availability of relevant firm produced social media analytics. Because SMA was held closely by companies as a proprietary asset for competitive advantage against competitors, researchers have traditionally had a hard time obtaining actual analytics for empirical study (Holsapple et al., 2018). Over time firms disclosed SMA in an effort to aid research that broadly assists society in developing solutions for example around pandemics(Poom et al., 2020; *Social Connectedness Index – Facebook Data for Good*, 2021). This study utilized data from these newer collaborations in order to overcome the access to SMA barrier. The second barrier involved users' lack of knowledge of SMA and therefore a lack of examination of their SMA privacy management expectations. This barrier was overcome recently as more SMA was released for public good and by firms exposing users to resources that demonstrated the processes that developed SMA and created intimate knowledge of it. To measure user knowledge, instrument items from the social science literature were adapted to measure their self-perception of intimate knowledge.

In addition to these barriers, the issue of lack of comprehensive frameworks to examine the intersection of user psychology around privacy and privacy decision making that involves multiple entities had long been acknowledged (Bélanger & Xu, 2015; Chen et al., 2017; Smith et al., 2011). This study proposed to overcome this issue by combining

constructs from a recently published theory for multilevel privacy decision making with established theories on psychological ownership in organizations (Bélanger & James, 2020; Pierce et al., 2001).

Assumptions, Limitations, and Delimitations

Measurements of constructs in the model were limited to a fixed point in time. The three key environment factors that Bélanger and James (2020) identified were location (virtual or physical), people presence (virtual, physical), and information (format, type, ownership perceptions). For purposes of SMA information privacy management, all other environmental characteristics were controlled for in order to examine the specific influence of intimate knowledge and co-ownership perception.

This study stood a realistic chance of resolving the influence of intimate knowledge and co-ownership perception on the constructs in TMIP since a previous correlation study had successfully used a similar approach to explain the influence of co-ownership perception of unanalyzed SM data on information privacy constructs, albeit in a different theoretical framework (Zhu & Kanjanamekanant, 2020). Zhu and Kanjanamekanant's (2020) study successfully tested the effect of co-ownership perception on information privacy decisions using communications privacy theory (CPM) from which TMIP was based. Additionally, another study successfully examined the influence of self-identity constructs in predicting organization ownership constructs in social media use (Karahanna et al., 2018). Intimate knowledge had also been shown to be part of the self-identity construct of co-ownership (Pierce et al., 2001). All the adapted constructs had previously been tested in SM studies. Changing the context to SMA and evaluating using a comprehensive model that combined the relevant constructs used previous studies had a

good chance of succeeding in explaining the relationship between constructs and contribute to the literature.

List of Acronyms

1. COP Co-ownership perception
2. CPM Communications Privacy theory
3. IPN Information privacy norms
4. IRB Nova Southeastern University institutional review board
5. IS Information systems
6. MIPD Multilevel information privacy decisions
7. MTurk Amazon Mechanical Turk
8. NAF Needs-affordances-features perspective on social media
9. PLS Partial least squares analysis
10. PO Psychological ownership
11. SCT Self-categorization theory
12. SM Social media
13. SMA Social media analytics
14. TMIP Theory of multilevel information privacy

Definition of Terms

Table 1 gives a definition of the terms in the proposed model and their prior use.

Table 1

Model Constructs Definition and Use in Prior Studies

Term	Definition	Prior study	Study description
Intimate knowledge	Knowledge of an object, person, or place, a fusion of the self with the object takes place (Beaglehole, 1932).	(Kwon, 2020)	Social media user participation
Co-ownership perception	View of which other entities may claim ownership and the weight assigned to each claim (Bélanger & James, 2020).	(Zhu & Kanjanamekanant, 2020)	Social media personal ad privacy
Social identity	"That part of an individual's self-concept that derives from his knowledge of membership of a social group or groups together with the emotional significance attached to that membership" (Tajfel, 1974, p. 69).	(Bagozzi & Lee, 2002; Bergami & Bagozzi, 2000; Tajfel, 1974; Tsai & Bagozzi, 2014)	Social identity, social media usage
Information privacy norm	Individual and group rules for managing information and interaction with others (Bélanger & James, 2020).	(Bélanger & James, 2020)	Theory development
Privacy calculus	Information privacy decisions are made based on a rational examination of costs and benefits of disclosure (Dinev et al., 2013).	(Krasnova & Veltri, 2010)	Social media, culture, and cost/benefit analysis
Multilevel information privacy decision	The application of the salient social identity IPNs to guide which information to disclose (Bélanger & James, 2020).	(Bélanger & James, 2020)	Theory development

Summary

In this chapter, the problem of users' low intimate knowledge of SMA and low co-ownership perception of SMA which lead to business disruptions were presented. A model for resolving this problem by combining classic constructs from the psychology of ownership literature with recent constructs of multilevel information privacy decision making in IS was outlined. Relevant hypotheses to empirically examine the impact of intimate knowledge on co-ownership perception were enumerated. In addition, the relationship between co-ownership perception's and three antecedents of SMA information privacy decisions: social identity, social norms, and the cost-benefit estimation in the privacy calculus were outlined. The relevance and significance to society and literature of resolving this problem was explained. Previous barriers and issues were presented along with the assumptions, limitations, and delimitations needed for this study. A definition of terms and acronyms used throughout the document were presented for convenience.

Chapter 2

Review of Literature

Overview

Because information privacy is studied in multiple disciplines, a classical three stage concept-centric literature review was performed. The review also used creativity methods to combine classic theories to form a theoretical foundation to examine the problem of interest (Watson & Webster, 2020; Webster & Watson, 2002). The theory underpinning multilevel information privacy management and psychological ownership in organization theory were used (Bélanger & James, 2020; Pierce et al., 2001).

In the first stage of the literature review, top information systems journals were searched for articles that mention “analytics” and “privacy”. In addition, journals in disciplines that were reported to often intersect with information systems in studying information privacy such as computer science, marketing, and the social sciences were searched (Smith et al., 2011). This resulted in 530 articles. The collection of journals searched are shown in Table 2.

The titles and abstracts of each of the articles were read to understand whether the article's problem of interest was information privacy for SMA. Articles found to only mention analytics and information privacy tangentially to their problems of interest were eliminated, resulting in ten articles from top information systems journals, five articles from marketing literature, and two recent SMA privacy review articles that covered computer science attempts at privacy preservation. The SMA privacy studies are shown

in Table 3. Table 4 shows the studies from information systems and Table 5 shows the reviews from computer science and the rest of the social science literature.

Table 2

Literature Review Sources

Information Systems	Marketing/Computer Science/Social Sciences
MIS Quarterly Information Systems Research, Management Science Journal of Management Information Systems Decision Sciences Communications of the ACM Decisions Support Systems European Journal of Information Systems Information and Management	Journal of Consumer Marketing Journal of Marketing Marketing Letters Marketing Education Review Journal of the Academy of Marketing Science Journal of Marketing Journal of Business Research Journal of Retailing Harvard Law Review Handbook of Theories of Social Psychology Retail Futures Privacy and Freedom
Information Systems Journal Journal of Decision Systems Journal of Information Privacy and Security Journal of Strategic Information Systems The Academy of Management Review Knowledge and Information Systems Information Sciences	Journal of Parallel Computing IEEE Communications Surveys & Tutorials Big Data and Society Computers in Human Behavior Journal of Parallel and Distributed Computing Network and Distributed System Security Symposium Foundations and Trends in Theoretical Computer Science World Wide Web IEEE Transactions on Dependable and Secure Computing Security and Communication Networks
International Conference on Information Systems	Journal of Social Issues Journal of Social Psychology Social Psychology Quarterly Social Science Research Network Science Scientific American

In the second literature review stage, articles referenced in the seventeen studies located in stage 1 were reviewed. The titles, keywords, and abstracts were read to determine whether any additional articles should be considered. Finally, in the third stage of the review, the web of science was used to search for any additional articles which mention analytics or privacy for any extra articles to include as recommended in the literature.

Even though the concepts from journals in several fields were reviewed, this study's definition of information privacy came from IS. Specifically, information privacy was defined as the ability to control information use about one's self rather than any other conceptualizations from other fields such as their use of physical privacy which refers to access to the individual's surroundings or private space (Bélanger & Crossler, 2011; Smith et al., 2011). Additionally, information privacy was reviewed as a cognitive state rather than as a value based one as embraced in other literature such as the law. Smith et al. (2011) outlined that privacy viewed from a value perspective was either defined as a right undergirded by laws or as a commodity to be traded for economic benefit. They established that most IS studies viewed information privacy as a cognitive situational state or one of the cognitive abilities to control the use of information about oneself. Like much of the information privacy research, this definition was adopted for this study.

Low social media analytics intimate knowledge and co-ownership perception among social media users lead to perceived lack of ability to control for unexpected privacy decisions which result in business disruptions (Acquisti et al., 2015; Bélanger & James, 2020; Yun et al., 2019). The IS literature classically defined information privacy as the

ability to control how and when one's personal information can be used (Bélanger & Crossler, 2011). Many IS studies define the ability to control this use as it was manifested in the form of disclosure decisions separately at either the individual, group, organization, or societal levels in spite existing calls for multi-level study (Laufer & Wolfe, 1977; Smith et al., 2011; Westin, 1967). Recent studies, however, recognized stakeholders' joint privacy decision interests across these levels and provide theoretical frameworks to explore their relevant constructs (Bélanger & James, 2020).

Increasingly, businesses used big data enabled analyzed information, such as social media analytics, to enhance their services (Kitchens et al., 2018). However, business use of analytics in particular had been associated with decisions that lead to a perceived loss of privacy and resulted in negative affective action by users (Bélanger & Crossler, 2019; Vannucci & Pantano, 2020). In the next three sections the existing studies in the IS literature on information privacy decision making, big data information privacy decision making in general, and social media analytics information privacy decision making are reviewed.

Theoretical Foundation

The origins of the IS information privacy definition begun with the general privacy definition in law as right to be let alone which included the protection of both intangible and tangible property articulated in nineteenth century law literature (Warren & Brandeis, 1890). The social sciences literature subsequently defined information privacy, from a cognitive perspective, as the claim of individuals, groups, and institutions to self-determine the extent of communication of information about themselves (Westin, 1967). Subsequent study builds on Westin's (1967) work to include the control construct as

crucial to information privacy (Altman, Irwing, 1975; Laufer & Wolfe, 1977). Current IS literature defined information privacy as the ability to control one's information in individual, group, organizational, and societal contexts (Bélanger & Crossler, 2011; Smith et al., 2011).

Existing Studies

The IS literature was the context for the SMA literature review with most relevant work appearing in the big-data analytics privacy stream. The main themes found in this stream were user awareness of analytics, user privacy consent, use implications, analytics privacy concerns, cost-benefits estimation in the privacy calculus, and algorithmic privacy preservation in analytics generation and dissemination. Table 3 outlines the studies and their relevant analytics privacy findings.

Table 3

Information Systems Analytics Privacy Literature Review

Journal	Authors	Analytics Privacy Findings
Communications of the Association of Information Systems	(Alashoor et al., 2017)	Awareness of big-data implications leads to higher privacy concerns.
Decision Support Systems	(Koh et al., 2017)	Privacy calculus' costs-benefits estimation primary driver of disclosure intentions in analytics over monetary inducements.
Decision Support Systems	(X.-B. Li & Raghunathan, 2014)	Novel economic incentive model for privacy consent adoption to minimize privacy violations.
European Journal of Information Systems	(Cheng et al., 2021)	Analytics privacy control and perceived benefits lead to higher service use.
Information Systems Research	(X.-B. Li & Sarkar, 2013)	Algorithmic privacy-preservation in analysis stage of analytics generation.
Information Systems Research	(X.-B. Li & Qin, 2017)	Algorithmic privacy-preservation in analysis stage of healthcare analytics generation.
Information Systems Research	(Kim & Kwon, 2019)	Algorithmic privacy-preservation in analysis stage of healthcare analytics generation: novel recursive partitioning.
MIS Quarterly	(X.-B. Li & Sarkar, 2014)	Algorithmic privacy-preservation in analytics: encryption de-identification, and anonymization.
MIS Quarterly	(Gopal et al., 2018)	Analytics disclosure intentions to third party sites moderated by levels of user privacy concerns.
MIS Quarterly	(Koh et al., 2017)	Analytics using sites need to reassure customers of privacy in order to maximize profits.

Many marketing studies commented on the importance of both general analytics and social media analytics' effect on user privacy violations perception and on effectiveness of marketing communications. However, theoretical and empirical studies where analytics information privacy was explored were limited to a few approaches. The main approaches advocated for behavioral choice and identity theory led information privacy management (Martin & Murphy, 2017), and that firms take action to raise user awareness of privacy policies (Bradlow et al., 2017; Corrigan et al., 2014), to obtain consent from users prior to analysis (Wieringa et al., 2021), and algorithmically preserve privacy in the collection, verification, and analytics generation. Marin and Murphy (2017) suggested as future areas of research a better examination of consumer choice related to firm information use. They also suggested that different individual's identities could have an important role in the analytics information privacy management. Their suggestions do not appear to have much empirical response in the analytics field and this study responded to their calls for future study. Table 4 shows articles in the marketing literature that examined analytics privacy.

Table 4

Marketing Analytics Privacy Literature Review

Journal	Author	Analytics Privacy Findings
Marketing Education Review	(Corrigan et al., 2014)	Encourage users to review company privacy policy for analytics privacy awareness.
Journal of the Academy of Marketing Science	(Martin & Murphy, 2017)	Advocate behavioral choice and identity theory led information privacy management.
Journal of Marketing	(Wedel & Kannan, 2016)	Algorithmic protection of information privacy
Journal of Business Research	(Wieringa et al., 2021)	Consent based, legal and algorithmic protection at collection, verification, storage, analytics generation, and dissemination.
Journal of Retailing	(Bradlow et al., 2017)	Opt-in privacy policy and increase user awareness of the value of predictive analytics

The computer science analytics privacy studies focused on algorithmic privacy protection methods, models and metrics in the various stages of analytics generation, publishing, and use. The methods used include those in anonymization of data, cryptography, perturbative methods that modify the input data to analytics, and non-perturbative ones that do not modify. Various anonymity, diversity, closeness and differential privacy models in analytics were utilized throughout. Finally, various studies present metrics to track likelihood of privacy preservation in the various stages of analytics generation and dissemination. Table 5 shows articles that covered many of these

algorithmic techniques to enable analytics information privacy from the computer science and social sciences literature.

Table 5

Computer Science and Social Science Analytics Privacy Literature Reviews

Analytics Stage	Privacy Risk	Analytics Privacy Approaches	Studies
Publishing	Individual user identity disclosure risk.	Anonymization based models	(Casas-Roma et al., 2017; Yang et al., 2014)
Publishing	Links between users' identity disclosure risk.	Anonymization and randomization-based models	(Blocki et al., 2013; Ying & Wu, 2011)
Publishing	Content disclosure risk.	Differential privacy and data perturbation.	(Dwork, 2011; Dwork & Roth, 2013; Zhang et al., 2018)
Querying	Search keyword disclosure risk.	Cryptographic approaches.	(Acar et al., 2018; Q. Wang et al., 2018; Zhao et al., 2019)
Querying	Querying user identity disclosure risk.	Cryptographic approaches.	(Acar et al., 2018; X. Wang et al., 2017; Zhao et al., 2019)
Data Mining	Input data disclosure.	Aggregation, Interference attack protection	(T. Li et al., 2018)
Data Mining	Data mining models disclosure.	Federated learning	(Shokri & Shmatikov, 2015)
Data Mining	Model output disclosure.	Cryptographic approaches	(Bost et al., 2015; Graepel et al., 2013)

Gaps in the Literature

This review of the relevant literature showed a gap that this study sought to address. The existing studies in the IS and related disciplines of computer science, marketing, and social science above showed analytics privacy focuses on individual-level and self-disclosure decisions (Bélanger & James, 2020). Across these multiple disciplines, analytics privacy was examined from singular perspectives either of individual or firm but not both. Each of the reviewed studies examined several SMA approaches; were users aware of analytics existence, did users understand the implications of its use, did users consent to the use of their data to creating analytics, which factors contributed to user privacy concerns in analytics, and which algorithmic methods did firms use to preserve privacy during the analytics generation and sharing processes. Most of the existing studies appeared to proceed under the assumption that users retain decision making on privacy for a while until they gave consent to the use of their information, shared their data, and their data was de-identified in readiness for analytics generation. Once firms removed personally identifiable information, then the user role in privacy appeared to no longer be present as the resulting analytics and its privacy management was presented as if it belonged solely to the firm. However, the CPM and its recent application in IS as the theory of multilevel information privacy called into question this assumption and contends that information contribution leads to continued co-ownership which then leads to a multi-level and joint privacy management (Bélanger & James, 2020). SMA information privacy decisions appeared to require further study as a multi-level concept even though privacy decisions that negatively impact stakeholders at both the individual and organization continued to be reported (Bélanger & James, 2020; Holsapple et al.,

2018). Most studies did not appear to empirically study the user and the organization's tandem social media analytics privacy management. This study looks to address this gap.

Synthesis

Identifying and measuring the factors that influence the user's most effective participation with the firm in SMA privacy decision management was the goal. The IS literature had clarified that information privacy closely related constructs of anonymity, secrecy, security, or ethics were not its equivalents (Dinev et al., 2013; Smith et al., 2011). Much of the reviewed literature from IS and computer science used algorithms to de-identify and anonymize SMA. Smith et al. (2011) cautioned that while anonymity and security have a role to play in privacy, they were not the whole picture when it comes to privacy. IS held that information privacy is the ability to control the use of one's information (Bélanger & Crossler, 2011; Smith et al., 2011). The goal was to suggest enhancements to user's contribution to the SMA privacy management with the hope of contributing a more robust approach to be used in tandem with existing practices. This approach contrasted with the approaches that sought to sufficiently eliminate stakeholder's personal stakes and to accord firms sole privacy rights as appeared to be the case with SMA. The relevant constructs that the literature identifies as antecedents for normative SMA multi-level information privacy decision making between the user and the firm in order to assuage perceived privacy violations and business disruptions were examined (Bélanger & James, 2020).

Summary

In this chapter, the information systems and related disciplines of marketing, computer science and social science literature were reviewed in order to surface what was known

about SMA information privacy management. While SMA information privacy was often commented upon in the literature, it appeared to need further empirical study. The studies that specifically covered SMA information privacy management were identified. From a review of these works, a gap in the study of joint user and firm SMA information privacy management was identified. Empirical study of constructs that are antecedents to an effective multilevel information privacy management were expected to contribute to the literature. Such a contribution was expected to go a long way in assuaging the negative affectations and business disruptions caused by perceived privacy violations brought on by non-normative SMA information privacy management.

Chapter 3

Methodology

Overview

In this chapter, the research design and methodology, instrument development, the proposed sample, data gathering and analysis, results formats, and resource requirements for the study, and a summary of the methodology used were presented. A theoretical model using psychological ownership in organizations theory and the theory of multilevel information privacy was built in order to examine the relationship between intimate knowledge of SMA and co-ownership perceptions of SMA and the antecedents of multilevel information privacy decisions: information privacy rules, salient social identity, and the cost-benefit components of the privacy calculus. Hypotheses based on the model were developed in order to that they be then tested using a web-based survey.

Research Methodology

Survey research to collect quantitative data was used. A survey was defined as a system for collecting information from individuals to explain their knowledge, attitudes and behavior (Fink, 2003). Fink (2003) outlined that the survey system should set data collection objectives, design the study, prepare a reliable and valid instrument, administer the survey, manage and analyze, and report the results. Survey research employs interviews, observation, and administered questionnaires to collect data (Sekaran & Bougie, 2019).

The data collection objectives were to collect SM user SMA intimate knowledge and resulting co-ownership of SMA. Co-ownership levels and SM user expectations of which

social identity and information privacy norms are used in privacy decision making were also to be collected. Finally, the last objective was to collect data on SM users' expectations of their involvement in the cost-benefit estimation in the privacy calculus and its impact on the use of norms to make the privacy decision. To design the study, measures were adopted from previous IS instruments that tapped the constructs of interest. Minor wording changes were made to make the question relevant to this study. The wording of questions, scaling of variables and general appearance was focused on as recommended in the literature (Sekaran & Bougie, 2019). As Sekaran and Bougie (2019) recommended, the questions wording was examined for content and purpose, wording and language, type and form, sequencing and personal information. The type and form of the question was examined for variations of positively and negatively worded questions, absence of double-barreled and ambiguous questions, removal of recall dependent, leading, and loaded questions. The wording was also be examined to ensure no questions were posed to elicit social desirable answers. The length of questions was minimized, and the questions sequenced from general to specific. Personal demographic questions were designed to keep the respondent anonymous, and this assurance was presented in the questionnaire.

A self-administered electronic questionnaire was used to collect data. This method was suitable as the respondents were distributed over the wide geographical area the study targeted. The electronic questionnaire was also anticipated to be inexpensive and convenient for the respondents. The typical disadvantages of this method such as low computer literacy and poor access to a computer (Sekaran & Bougie, 2019) were less of a concern since the respondents were pre-screened for familiarity with SM use which

requires computer literacy and technology access. To increase responses a small fee for filling the survey was paid for completing the survey. This study used the Qualtrics online survey provider to administer an electronic questionnaire. Qualtrics was used because it was much easier to access, administer, and complete than a printed survey (Bryman, 2012). Qualtrics also allowed for anonymous integration with Amazon's Mechanical Turk (MTurk), the crowdsourcing platform used. MTurk had been accepted as a demographically diverse source of quality and reliable behavioral research data that improved considerably over convenience sampling (Lowry et al., 2016; Mason & Suri, 2012). MTurk was used to find participants and administer the actual study. A small fee of less than $0.30 was paid to survey respondents to complete the survey. Only MTurk respondents with a Facebook account and with high approval ratings above 95% were allowed to take the survey. The respondents were asked a question about their frequency of Facebook use. Only those with an active Facebook account and who had used it in the month prior were included in the survey results. After administering the survey, Qualtrics was also be used to manage and preliminarily analyze survey results.

Instrument Development

All the survey measurement items were adopted from items used in previous studies in the literature. In developing the survey instrument, only small wording changes were made to each scale to contextualize the questions to this study's goals. Appendix A details the questionnaire used to measure each construct. Table 6 summarizes the source for each scale for each construct in this study's model.

This study conducted a pilot test of the survey using 34 participants. The participants were a convenience sample of family members, friends, and participants from network of

the researcher. Feedback obtained from the pilot study was used to clarify and improve wording for the study on the study.

The smart partial least squares 3 software package (SmartPLS) was used to test for reliability of the constructs using established thresholds (Durcikova et al., 2018; Nunally, 1978; Ringle et al., 2012). Ringle (2012) detailed three criteria to provide evidence of the reliability of the constructs. First, item loadings in partial least squares were checked to ensure they were above 0.7 cutoff. Second, internal consistency was evaluated using composite reliability to ensure their values exceed Nunally's (1978) 0.7 cutoff. Finally, the average variance extracted was calculated and checked to exceed Chin's (1998) cutoff of 0.50 for average variance.

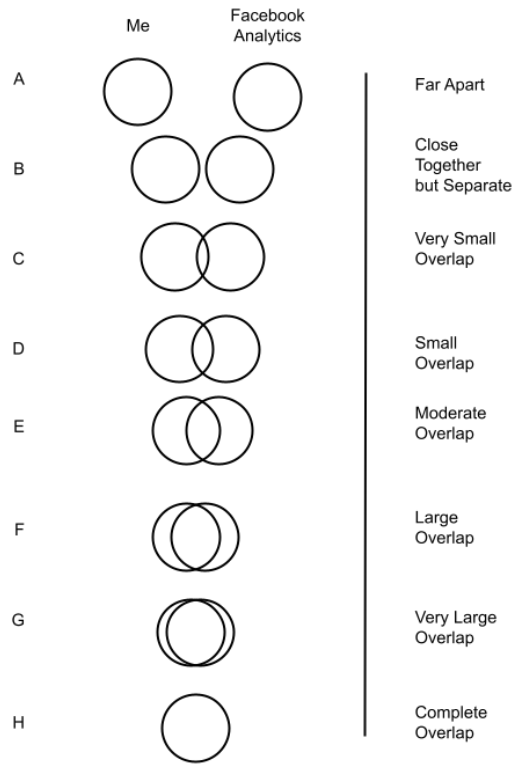
SmartPLS was used to calculate values which were also used to test the measurement model indicator loadings, internal reliability, convergent reliability and discriminant reliability (Hair et al., 2019). Cronbach's alpha test in SmartPLS was used to test the salient social identity and information privacy rule items. Cronbach's alpha above 0.80 were sought for tests to establish good inter item consistency (Hair et al., 2011). A popular approximately exact measure of construct reliability ρ_A was also calculated (Dijkstra & Henseler, 2015). The results from the study were used to perform factor analysis using the SmartPLS software to establish construct validity.

The intimate knowledge construct was measured using a scale originally utilized in the marketing literature and also used in an empirical IS research (Kent & Allen, 1994; Kwon, 2020). A seven-point Likert scale ranging from 1 (unfamiliar/inexperienced/not knowledgeable) to 7 (familiar/experienced /knowledgeable) was used in this scale. The co-ownership perception construct was measured using three scales adopted from IS

organization studies (Jarvenpaa & Staples, 2001; Zhu & Kanjanamekanant, 2020). The co-ownership perception scales use five-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree). Two scales to measure cognitive social identity developed in the psychology literature and used in a leading IS study (Bergami & Bagozzi, 2000; Tsai & Bagozzi, 2014) were used. The scale adopted from Bergami and Bagozzi (2000) that measured the degree of social identity overlap is illustrated in Figure 2. Bergami and Bagozzi (2000) and Tsai and Bagozzi (2014) used variations of this visual scale to measure respondents' organization self-identification. This scale was useful in that it enabled the measurement of users' self-identification overlap with the group social identity resulting from co-ownership perception.

Figure 2

Self-definition and Organization Social Identity Overlap



Note: Self-definition and organization social identity overlap. Adapted from "Self-categorization, affective commitment and group self-esteem as distinct aspects of social identity in the organization," Bergami and Bagozzi, 2000, *British Journal of Social Psychology, 39*(4), p. 575. Copyright 2000 by the British Psychological Society.

To measure the information privacy norms, eighteen scales used in prior IS studies to measure privacy rule development were adopted (Child et al., 2009; Hollenbaugh, 2019). Child et al. (2009) developed and validated an information privacy norm development instrument. Their instruments used six scales each to measure the three factors that impact collective privacy boundaries key to information privacy norm formation:

ownership, boundary permeability, and boundary linkages. Three scales for costs and four for benefits in the privacy calculus estimation were adopted from the IS literature (Dinev et al., 2013). Finally, the "We-intentions" scales previously used in IS to measure expectations for joint privacy decision making were used (Tsai & Bagozzi, 2014).

Table 6

Summary of Measures

	Construct	Measure	Source
IKN1	Intimate knowledge	Regarding the services offered from Facebook Social Connectedness Index (SCI), are you. (7-point "unfamiliar - familiar")	(Kent & Allen, 1994; Kwon, 2020)
IKN2	Intimate knowledge	Regarding the services offered from Facebook Social Connectedness Index (SCI), are you. (7-point "inexperienced - experienced")	(Kent & Allen, 1994; Kwon, 2020)
IKN3	Intimate knowledge	Regarding the services offered from Facebook Social Connectedness Index (SCI), are you. (7-point "not knowledgeable - knowledgeable")	(Kent & Allen, 1994; Kwon, 2020)
OWNSP1	Co-ownership perception	I feel Facebook has the right to use the Social Connectedness Index. (5-point "strongly disagree - strongly agree")	(Jarvenpaa & Staples, 2001; Zhu & Kanjanamekanant, 2020)
OWNSP2	Co-ownership perception	I feel the Social Connectedness Index belongs to Facebook too. (5-point "strongly disagree - strongly agree")	(Jarvenpaa & Staples, 2001; Zhu & Kanjanamekanant, 2020)

(continued)

Table 6 (continued)

Summary of Measures

	Construct	Measure	Source
OWNSP3	Co-ownership perception	I feel Facebook and I co-own the Social Connectedness Index. (5-point "strongly disagree - strongly agree")	(Jarvenpaa & Staples, 2001; Zhu & Kanjanamekanant, 2020)
SIC1	Social identity - cognitive	How would you express the degree of overlap between your personal identity and the identity of a joint (Facebook and you) group formed to manage Social Connectedness Index privacy decisions? (8-point graphical "not at all -very much" scale)	(Bergami & Bagozzi, 2000; Tsai & Bagozzi, 2014)
SIC2	Social identity cognitive	Please indicate to what degree your self-image overlaps with the identity of the joint group as you perceive it (7-point "not at all - very much" scale)	(Bergami & Bagozzi, 2000; Tsai & Bagozzi, 2014)
IPNP1	Information privacy norm - boundary permeability	When I face challenges in my life, I feel comfortable talking about them on my Facebook account that is used to create SCI analytics. (7-point "not at all - very much" scale)	(Child et al., 2009; Hollenbaugh, 2019)
IPNP2	Information privacy norm - boundary permeability	I like my Facebook entries to be long and detailed on the Facebook account that is used to create SCI analytics. (7-point "not at all - very much" scale)	(Child et al., 2009; Hollenbaugh, 2019)
IPNP3	Information privacy norm - boundary permeability	I like to discuss work concerns on my Facebook account that is used to create SCI analytics. (7-point "not at all - very much" scale)	(Child et al., 2009; Hollenbaugh, 2019)
IPNP4	Information privacy norm - boundary permeability	I often tell intimate, personal things on my Facebook account that is used to create SCI analytics without hesitation. (7-point "not at all - very much" scale)	(Child et al., 2009; Hollenbaugh, 2019)

(continued)

Table 6 (continued)

Summary of Measures

	Construct	Measure	Source
IPNP5	Information privacy norm - boundary permeability	I share information with people whom I don't know in my day-to-day life. (7-point “not at all - very much” scale)	(Child et al., 2009; Hollenbaugh, 2019)
IPNP6	Information privacy norm - boundary permeability	I update my Facebook account that is used to create SCI analytics frequently. (7-point “not at all - very much” scale)	(Child et al., 2009; Hollenbaugh, 2019)
IPNO1	Information privacy norm - boundary ownership	I have limited personal information on my Facebook account that is used to create SCI analytics. (7-point “not at all - very much” scale)	(Child et al., 2009; Hollenbaugh, 2019)
IPNO2	Information privacy norm - boundary ownership	I use shorthand (e.g. pseudonyms or limited details) when discussing sensitive information on my Facebook account that is used to create SCI analytics. (7-point “not at all - very much” scale)	(Child et al., 2009; Hollenbaugh, 2019)
IPNO3	Information privacy norm - boundary ownership	If I think that the information I posted on my Facebook account that is used to create SCI analytics really looks too private, I might delete it. (7-point “not at all - very much” scale)	(Child et al., 2009; Hollenbaugh, 2019)
IPNO4	Information privacy norm - boundary ownership	I usually am slow to talk about recent event on my Facebook account that was used to create SCI analytics because people might talk. (7-point “not at all - very much” scale)	(Child et al., 2009; Hollenbaugh, 2019)
IPNO5	Information privacy norm - boundary ownership	I don't post on my Facebook account that is used to create SCI analytics about certain topics because I worry about who has access. (7-point “not at all - very much” scale)	(Child et al., 2009; Hollenbaugh, 2019) (continued)

Table 6 (continued)

Summary of Measures

	Construct	Measure	Source
IPNO6	Information privacy norm - boundary ownership	Seeing intimate details about someone else through my Facebook account that is used to create SCI analytics makes me feel I should take step to keep their information private. (7-point "not at all - very much" scale)	(Child et al., 2009; Hollenbaugh, 2019)
IPNL1	Information privacy norm - boundary linkages	I accurately update the profile on my Facebook account that is used to create SCI analytics so others can find me. (7-point "not at all – very much" scale)	(Child et al., 2009; Hollenbaugh, 2019)
IPNL2	Information privacy norm - boundary linkages	I try to let people know my best interests on my Facebook account that is used to create SCI analytics so we can be friends. (7-point "not at all - very much" scale)	(Child et al., 2009; Hollenbaugh, 2019)
IPNL3	Information privacy norm - boundary linkages	I allow people with a profile that I don't know to have access to my Facebook account that is used to create SCI analytics. (7-point "not at all - very much" scale)	(Child et al., 2009; Hollenbaugh, 2019)
IPNL4	Information privacy norm - boundary linkages	I comment on others Facebook posts to have others check out my Facebook account that is used to create SCI analytics. (7-point "not at all - very much" scale)	(Child et al., 2009; Hollenbaugh, 2019)
IPNL5	Information privacy norm - boundary linkages	I allow anonymous access to my Facebook account that is used to create SCI analytics. (7-point "not at all - very much" scale)	(Child et al., 2009; Hollenbaugh, 2019)
IPNL6	Information privacy norm - boundary linkages	I regularly make friend requests to interesting profiles to increase traffic to the Facebook account that is used to create SCI analytics. (7-point "not at all - very much" scale)	(Child et al., 2009; Hollenbaugh, 2019) (continued)

Table 6 (continued)

Summary of Measures

	Construct	**Measure**	**Source**
PCC1	Privacy calculus cost	In general, it would be risky to disclose personal information on my Facebook account that is used to create SCI analytics. (7-point "not at all - very much" scale)	(Dinev et al., 2013)
PCC2	Privacy calculus cost	There would be high potential for privacy loss associated with giving my personal information on my Facebook account that is used to create SCI analytics. (7-point "not at all - very much" scale)	(Dinev et al., 2013)
PCC3	Privacy calculus cost	Personal information on my Facebook account that is used to create SCI analytics could be inappropriately used	(Dinev et al., 2013)
PCC4	Privacy calculus cost	Providing personal information on my Facebook account that is used to create SCI analytics would involve many unexpected problems. (7-point "not at all - very much" scale)	(Dinev et al., 2013)
PCB1	Privacy calculus benefit	Revealing personal information on my Facebook account that is used to create SCI analytics will help me obtain information/products/services I want. (7-point "not at all - very much" scale)	(Dinev et al., 2013)
PCB2	Privacy calculus benefit	I need to provide my personal information on my Facebook account that is used to create SCI analytics so I can get what I want from Facebook. (7-point "not at all - very much" scale)	(Dinev et al., 2013)

(continued)

Table 6 (continued)

Summary of Measures

	Construct	Measure	Source
PCB3	Privacy calculus benefit	I believe that as a result of my personal information disclosure on my Facebook account that is used to create SCI analytics, I will benefit from a better, customized service and or better information and products. (7-point "not at all - very much" scale)	(Dinev et al., 2013)
PDN1	Privacy decision norm - We intentions	I intend that the group [i.e. Facebook and I identified as a group prior] manage the privacy of the analytics generated from my Facebook account in the next (5-point "disagree-agree" scale)	(Bagozzi & Lee, 2002; Tsai & Bagozzi, 2014)
PDN2	Privacy decision - We intentions	We [i.e. Facebook and I identified as a group prior] will jointly manage the privacy of the analytics generated from personal information from my Facebook account. (5-point "disagree-agree" scale)	(Bagozzi & Lee, 2002; Tsai & Bagozzi, 2014)

Instrument Revision

A pilot test with a convenience sample of 34 participants was conducted. The responses from the pilot test were used to revise the instrument. The instrument scales were revised based on feedback. Actual study data obtained was used to conduct exploratory factor analysis in the SmartPLS software.

Data Collection Procedure

Prior to collecting any data from human subjects, the instruments and protocols for this study were submitted to the Nova Southeastern University's (NSU) Institutional

Review Board (IRB). Once IRB approval was obtained, respondents were presented with NSU consent to participant letter for anonymous surveys. A sample consent form for all study participants is included in Appendix A.

A pilot study was conducted to collect data and feedback on the study instrument. The pilot study consisted of 34 participants selected from the researcher's family members, and friends. Potential participants were asked questions to ensure active Facebook usage and non-participation in Amazon MTurks service. 34 participants were identified and reviewed the survey that asks additional questions about the levels of intimate knowledge of several types of SMA. The pilot study participants were asked to review the survey questionnaire and to respond to each item while making notes for feedback on any of the items. After analysis, feedback from the pilot study was used be used to update and finalize the survey instrument.

The final survey was distributed electronically to respondents using the Qualtrics survey system and Amazon MTurk integration. Study participants read the directions and responded to the questionnaire's questions relevant to the constructs of interest. Study participants completed the survey describing their intimate knowledge of, co-ownership perception, social identities in relation to the decision to disclose their social connectivity index (SCI) analytics, their social privacy norms, their cost and benefit estimations in the privacy calculus, their expectations of information privacy norms, and their expectations for the privacy decisions to be made relative to the SMA they were most familiar with. The participants were then be asked to respond to questions that collect demographic data including age, income, education, and the levels of social media use.

Resource Requirements

An Internet-connected computer was needed to conduct this research. The software on it included the Microsoft word document processor, and the Zotero references management software. In addition, SmartPLS data analysis software was used for analysis. Survey items from the social sciences literature were obtained to measure SMA intimate knowledge, co-ownership perception, the cost and benefit concepts of the privacy calculus, salient social identity, and information privacy norms, privacy decision expectations. The wording from survey items previously used in the literature formed the basis of the wording for creating the survey instrument for data collection. The Qualtrics survey service and an online account to access Amazon's MTurk crowdsourcing service were used to administer the questionnaire and aid in data collection. Approximately 700 dollars was needed to pay for a Qualtrics license, SmartPLS 3 license, and Amazon MTurk usage for this study. The researcher provided funding for the various services and software licenses.

Nova Southeastern University's Alvin Sherman Library was used as a resource to retrieve the publications used in this research. The Nova Southeastern University institutional review board (IRB) provided the approval for the use of the survey questionnaire to collect data from human participants.

Summary

This chapter introduced the proposed research methodology, the research methods concepts and their implementation, instruments development and validation, the pilot sample, the study sample, the data collection procedure, the data analysis, and the various resource requirements.

Chapter 4

Results

Overview

The quantitative analysis of the data collected are presented in this chapter in four sections in order to answer the research question. First, the demographics of the study sample are presented in detail. In the second section, data analysis that includes the results of testing the measurement model, the structural model, and hypotheses are presented. Third, the findings from the hypotheses testing are discussed. Finally the chapter concludes with a summary of the results

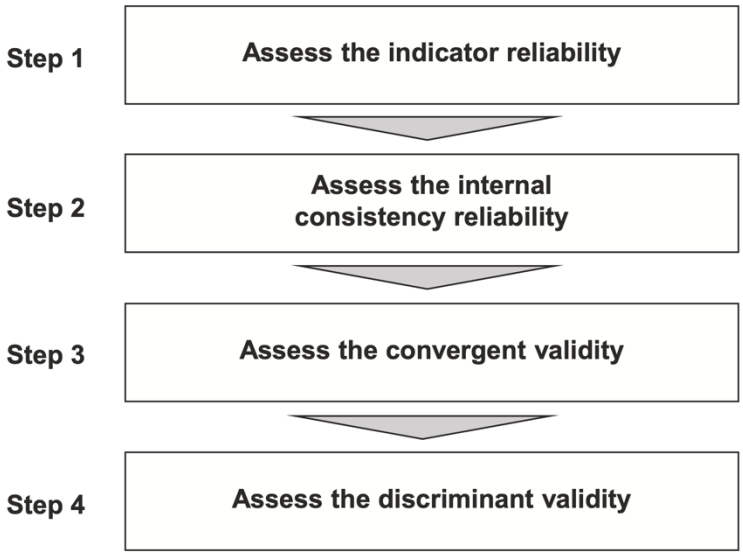
The demographics section presents the respondents demographic characteristics. These characteristics are important to addressing the research question since the theory of multi-level information privacy identifies various demographic factors as environmental characteristics that influence privacy decision making (Bélanger & James, 2020). The demographic characteristics are age, gender, race, level of education, state of residence in the United States, income level, and social media use. The results of the study are relevant to the sample demographics of interest.

Established methods for data analysis for the research model were selected and conducted and are presented. The model and scale developed to study the question of interest is reflective since all the items in the scale shared the information privacy decision construct as the common construct of interest (Sekaran & Bougie, 2019). Consistent with evaluation of this reflective research model, the validity and reliability of the measurement and structural model were determined. Four successive steps were used to assess the measurement model (Hair et al., 2022; Sekaran & Bougie, 2019). Per Hair et

al. (2022) recommendations indicator reliability was first established, then internal consistent reliability was measured, next the convergent reliability shown, and finally the discriminant validity was proven. Figure 3 shows the four recommended steps that were used to assess the measurement model.

Figure 3

Measurement Model Assessment



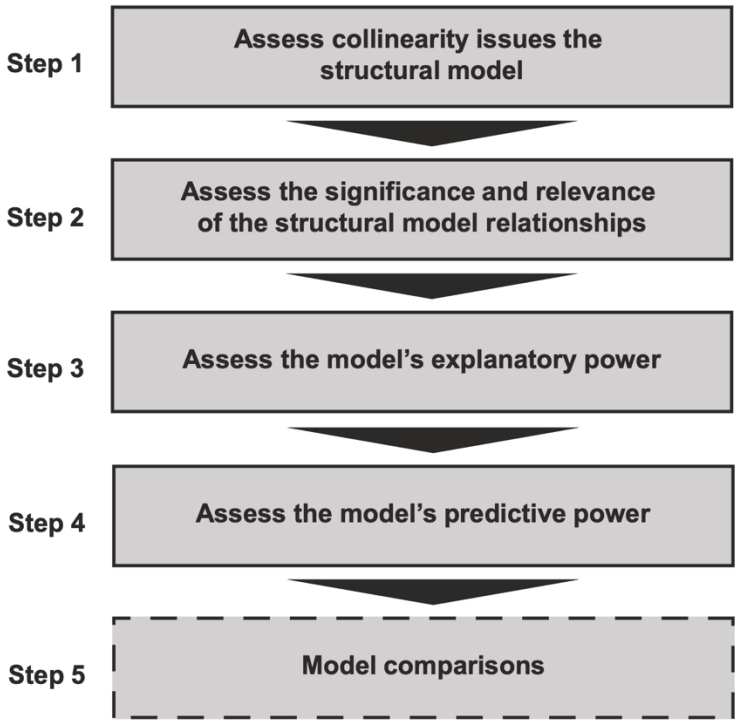
Note: Steps to assess the measurement model. Adapted from "Partial Least Squares Structural Modeling (PLS-SEM) using R," (p. 76), J. F. Hair, G. Tomas, M. Hult, C. M. Ringle, M. Sarstedt, N. P. Danks, and R. Soumya, 2022, Springer. Creative Commons License.

As recommended in the literature once the reliability and validity of the measurement model was established, the structural model was assessed next (Hair et al., 2019, 2022). Hair et al.'s (2022) steps for assessing the structural model were used to evaluate this study's model. First, the structural model was checked for collinearity issues. Second, the

structural model relationships were checked for significance and relevance. Third, the structural model's explanatory power was checked. Fourth, the structural model's predictive power was checked. Figure 4 shows the four steps that were taken to assess the structural model. Hair et al. (2022) left step 5 as optional for PLS-SEM analysis like ours that is not considering multiple models and this step was not performed.

Figure 4

Structural Model Assessment



Note: Steps to assess the structural model. Adapted from "Partial Least Squares Structural Modeling (PLS-SEM) using R," (p. 116), J. F. Hair, G. Tomas, M. Hult, C. M. Ringle, M. Sarstedt, N. P. Danks, and R. Soumya, 2022, Springer. Creative Commons License.

In step 1, the variance inflation factor (VIF) was calculated and compared to established thresholds in order to check for multicollinearity. The variance inflation factor determined the degree to which one variable is explained by another (Hair et al., 2019). Once collinearity was eliminated as a problem, bootstrapping was run to assess the path coefficients significance and relevance and that the values fall in an acceptable range in step 2 (Hair et al., 2019). In step 3, the variance of endogenous constructs which is the model's explanatory power were examined using coefficient of determination (R^2). Finally, in step 4 the model's predictive power $Q^2_{predict}$ was tested using PLS predict procedure in SmartPLS.

The analysis results are described and presented next in aggregate and summary formats. These formats include tables and descriptions summarizing the demographics of the study respondents, validity and reliability measures, moderation effects, and whether the hypotheses were supported and corresponding coefficients. A discussion of these results concludes this chapter.

Sample Characteristics

Sampling is the process of selecting a sufficient number of participants with enough properties and characteristics to allow generalization about the study population (Sekaran & Bougie, 2019). Sekaran and Bougie (2019) outlined that the sampling process involves defining the population, the sample frame, determining the sample design, setting the sample size and executing the sampling process.

Because the impact of intimate knowledge and co-ownership perception on the antecedents of social media analytics information privacy decisions in the US was this study's interest, the population chosen was the adult users of Facebook in the United

States. Facebook was the most popular leading social media platform whose SMA was readily available for study (Auxier & Anderson, 2021). Sekaran and Bougie (2019) explained that the sampling frame is a representation of all the elements in the population. The adult Facebook population has been approximated by the Pew research center at 178.2 million in 2021 which forms the frame for this study (Auxier & Anderson, 2021). The two major approaches to sampling reported in the literature are random and nonrandom sampling (Sekaran & Bougie, 2019; Terrell, 2015). Quantitative studies generally use random samples to increase the generalizability of the findings (Terrell, 2015). Random sampling was therefore used in this study.

Prior social science guidelines stated the sample minimum should follow the 10 times rule which has the minimum as the larger of 10 times the number of structural paths to any construct in the model or 10 times the number of formative indicators to measure a construct to avoid type II errors (Hair et al., 2022). For the model this means at least 100 participants. A priori sample size calculations using G*Power power analysis program for a medium effect at 0.80 power when significance is at 5 percent ($\alpha = 0.05$) for the correlation study is 64 (Faul et al., 2009).

The survey was distributed online, and the number of accepted responses was 372. This response quantity was well over both required sample size minimum guidelines with relatively low financial cost and was consistent with high reported response rates of above 90% for MTurks of similar recruitment profile in a previous study (Kwon, 2020). The 372 accepted responses demographic data were summarized using Qualtrics summaries. 49% of respondents identified as male, 50% as female, less than 1% as non-binary, and less than 1% preferred not to say. Two age groups, 25-34 (40%) and 35- 44

(27%), represented most of the respondents. The 18-24 (5%), 45-54 (13%), 55- 64 (9%), and 65 years and older (7%) age groups represented the remainder. Most of the respondents were white (81%). The rest of the respondents were Black/African American (7%), multi-racial (7%), Hispanic (2%), Asian (2%), and all others 1% or less. More than half of the respondents' highest level of education was a bachelor's degree (53%). Master's degree respondents constituted 21%, high school graduates (10%), some college but no degree (8%), associate degree (6%). Respondents with a less than a high school degree represented 1% and those with doctoral degree represented the remaining 1%.

The states with the highest representation were Indiana (15%), California (13%), and Texas (8%). All other states had 5% and below representation, with respondents from 47 different states. The most reported household earnings were $40,000-49,000 (17%), $50,000-59,000 (15%), $60,000 - $69,000 (10%). Each of the other income brackets reporting less than 10%. Facebook was the most often used social media platform among respondents at 73%. Instagram (17%), Twitter (6%), other platforms were reported at 4%. Most respondents reported checking Facebook very often: 28% reported checking more than 5 times a day, 27% reported checking 2-3 times a day, and 16% reported checking once a day.

Data Analysis

The collected data was analyzed in order to answer the question of what impact intimate knowledge and co-ownership perception have on the constructs that influence SMA information privacy decisions. Structural equation modeling (SEM) has been reported to be a powerful statistical tool for analyzing quantitative studies such as this whose models have several parts and whose dependent variables subsequently became

the independent variables for other relationships in the model (Hair et al., 2011, 2022). Hair et al. (2022) elaborate that SEM has two complimentary statistical methods covariance based (CB) and partial least squares (PLS). They reported that CB is typically used when the primary research objective is the validation of a concise research model and partial least squares is typically used when prediction and explanation is the aim. We used partial least squares since prediction and explanation of the impact intimate knowledge and co-ownership perception on the antecedents of normative SMA information privacy decisions was the study goal.

Partial least squares structural equation modeling (PLS-SEM) was chosen as it is widely used in the IS literature to evaluate the theory, model, and data in a complex causal study that extends existing theory such as this one (Aguirre-Urreta & Rönkkö, 2018; Hair et al., 2019). Additionally, PLS-SEM was well suited for this analysis given the small dataset (Chin, 1998). SmartPLS 3 is a popular comprehensive software tool for PLS-SEM (Hair et al., 2022; Sarstedt & Cheah, 2019). SmartPLS software has a graphical user interface that is used to perform variance based partial least squares structural equation modeling. To perform this analysis, Qualtrics survey data was downloaded and imported into SmartPLS software projects in comma delimited format with indicator labels forming the first row of the file and all other entries coded to integer values in successive rows (Wong, 2019). A project model was built in SmartPLS for the inner model and outer model by following Wong's (2019) recommendations for using the software package user interface and the model of the study. The inner model was built in SmartPLS user interface by clicking insertion mode, clicking in the interface to create circles that represent the latent constructs in this study, and labeling the constructs. The

relationships between the constructs were created in the project by switching to connection mode and dragging directional arrows to connect the constructs using the hypothesized relationships. The outer model was then built by clicking the indicator tab and dragging each indicator to its corresponding constructs. The study model was presented in Figure 5.

Once the model was built in SmartPLS, various user interface menus were used to configure and ran the various tests to validate the structural model and the measurement model. SmartPLS software allowed for the export of the output of the various algorithm results in comma delimited format which was then reported in this report. SmartPLS was chosen as the tool for partial least squares analysis for its ease of use and because it implements recent PLS techniques from the literature (Sarstedt & Cheah, 2019). The recommended PLS-SEM procedures for model and hypothesis testing were used for measurement model testing, structural model testing, and hypothesis testing (Hair et al., 2019). Per Hair et al. (2019) recommendations, model measurement testing included item reliability, internal consistent reliability, convergent reliability, and discriminant validity testing. As they recommended, once the measurement model was established as satisfactory, structural model testing was done. The structural model tests included collinearity tests, statistical significance and relevancy tests, model explanatory power tests, and model predict power tests. The measurement model testing is described in the next section followed by structural model testing.

Measurement Model Testing

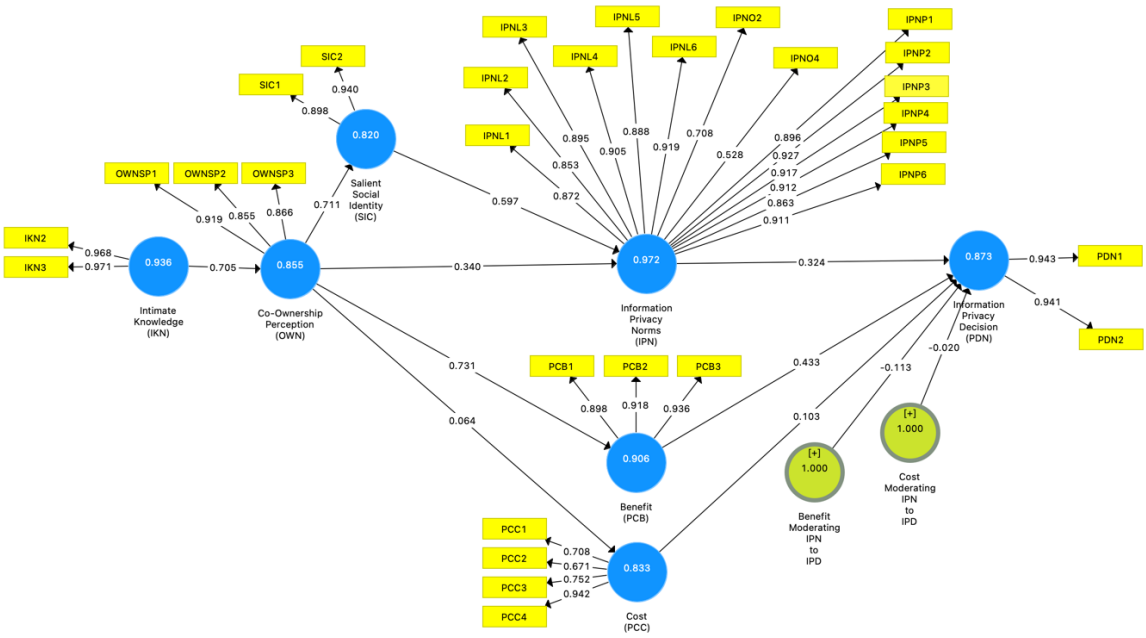
Four successive tests are commonly accepted in order to test the measurement model (Hair et al., 2019). Hair et al. (2019) explained that the first test for item reliability

examines the indicator loadings to ensure they explain at least 50% of the construct's variance. They then detail that the second test checks internal consistency of the model by examining Cronbach's alpha against accepted thresholds. Their third test examines how the construct converges to explain the variance of its items in order to establish convergent validity. They concluded the validation of the measurement model with the fourth and final step that examines the heterotrait-monotrait (HTMT) ratio of the correlations in order to establish discriminant validity. These four tests were conducted for our analysis and the details are reported in the next few paragraphs.

First to test for item reliability, indicator loadings >= 0.708 are typically preferred to ensure each constructs explains more that 50% of the indicators variance in order to establish item reliability (Hair et al., 2019). However when the study is a theory extending exploratory study such as this one, a commonly acceptable >= 0.50 threshold is allowed (Bagozzi & Yi, 1988; Hair et al., 2019). SmartPLS partial least squares algorithm was run against our model and the collected data. 30 of the original 35 items in the model loadings were between the recommended 0.708 and the 0.95 thresholds. Items IPNO1, IPNO3, IPNO5, IPN06 with loadings lower than the 0.50 threshold (0.36, 0.206,0.286, 0.3.3) and IKN1 with a very high loading were dropped from the model. The dropped items constitute less than the 20% model change threshold that would otherwise cause content validity concerns and necessitate new data collection (Hair et al., 2022). Item reliability for the remaining items were established with the loadings demonstrated in Figure 5 that surpass acceptable thresholds to establish item reliability.

Figure 5

Measurement model - outer loadings, path co-efficient, Cronbach's alpha



As Hair et al. (2019) recommended, once item reliability was established, the second measurement model test examined internal consistent reliability. Internal consistent reliability measures how well the indicators for a construct are associated with one another (Hair et al., 2022). SmartPLS partial least squares algorithm was used to obtain values for internal consistent reliability. Internal consistent reliability ρ_A is an approximately exact measure of construct reliability which usually lies between Cronbach's alpha and composite reliability (Dijkstra & Henseler, 2015; Hair et al., 2019). ρ_A between 0.70 and 0.90 is recommended (Hair et al., 2019). Hair et al. detailed that reliability values of 0.95 are problematic and may indicate that items are redundant or have undesirable response patterns such as straight-lining. However, when the calculation produces ρ_A is above 1 as happened in this analysis, an error has occurred and its

recommended to return to Cronbach's alpha value (Sarstedt et al., 2020; Wong, 2019). Hair et al. (2022) detail that Cronbach's alpha is a conservative acceptable measure of internal consistent reliability which assumes the same thresholds as ρ_A. All items except the IPN construct in Table 7, showed Cronbach's alpha values above the 0.708 threshold. Intimate knowledge had a Cronbach's alpha of 0.936, co-ownership perception's was 0.855, salient social identity's was 0.82, information privacy norms' were 0.972, benefit in the privacy calculus' was 0.906, cost estimate in the privacy calculus' was 0.833, and information privacy decisions value was 0.888.

Table 7

Internal Consistent Reliability – Cronbach's Alpha

	Construct	**Cronbach's alpha**
IKN	Intimate Knowledge	0.936
OWN	Co-Ownership Perception	0.855
SIC	Salient Social Identity	0.82
IPN	Information Privacy Norms	0.972
PCB	Privacy Calculus Benefit	0.906
PCC	Privacy Calculus Benefit Cost	0.833
PDN	Information Privacy Decision	0.888

The IPN construct had a high value of 0.972 potentially raising three concerns about extremely high reliability raised in the literature: semantic redundancy, construct domain redundancy, and inappropriate data collection (Hair et al., 2019). The IPN items in question were not semantically similar and measured three different aspects of the information privacy norm construct's domain: ownership, boundary permeability, and

boundary linkages (Child et al., 2009; Dinev et al., 2013; Hollenbaugh, 2019). In addition, the collected data showed no signs of inappropriate data collection such as answers to the questions blocks having high internal data consistency. IPN construct item's validity was established as the construct's measurement overcame these three common concerns. The measurement model's internal consistent reliability was therefore established.

Once internal consistent reliability is established, Hair et al.'s (2022) third recommended measurement model test is convergent validity. Convergent validity is a measure of how much the indicators used to measure a construct are correlated and is measured using the average variance of extraction (AVE) (Hair et al., 2022). Their recommended value of AVE >= 0.50 was calculated and used to determine convergent validity. SmartPLS partial least squares algorithm was used to obtain AVE values. All constructs had acceptable AVE values >= 0.50. The various average variance extracted values were intimate knowledge (AVE=0.940), co-ownership perception (AVE=0.776), salient social identity (AVE=0.846), information privacy norms (AVE=0.745), benefit estimate in privacy calculus (AVE=0.842), costs estimate in the privacy calculus(AVE=0.601) and expected information privacy decision (AVE=0.888) . Table 8 shows a summary of the constructs AVE values. Since all constructs AVE were above the recommended threshold convergent validity for the measurement model was established.

Table 8

Convergent Validity – Indicators Average Variance Extracted

	Construct	Average Variance Extracted
IKN	Intimate Knowledge	0.940
OWN	Co-Ownership Perception	0.776
SIC	Salient Social Identity	0.846
IPN	Information Privacy Norms	0.745
PCB	Privacy Calculus Benefit	0.842
PCC	Privacy Calculus Benefit Cost	0.601
PDN	Information Privacy Decision	0.888

The final recommended test to validate the measurement model is discriminant validity (Hair et al., 2019). Hair et al. (2019) explained that discriminant validity measures how much the indicators used to measure one construct differ and are uncorrelated from the measures of other constructs using the Heterotrait-monotrait (HTMT) ratio. HTMT measures the mean correlations across constructs relative to the geometric mean of the average correlations for the items measuring the same construct (Henseler et al., 2015). HTMT <= 0.90 was the recommended value to establish discriminant validity (Hair et al., 2019).

Some HTMT values in this study were above the threshold. Per Henseler et al.'s (2015) guidance for this occurrence, HTMT was bootstrapped using SmartPLS to test that the HTMT was different than 1. Complete bootstrapping with 5,000 subsamples, one tailed test with a significance of 0.05 was done using the percentile method. The results

of the test are shown in Table 9 and all values were less than 1, establishing discriminant validity.

The measurement model's assessment was satisfactory with item reliability, internal consistent reliability, convergent reliability, and discriminant validity testing established. The structural model assessment was performed and is described next.

Table 9

Discriminant Validity – Bootstrapped HTMT Confidence Intervals

	Original Sample Mean	Bootstrapped Sample Mean	5%	95%
IPN leads to PCB	0.929	0.929	0.905	0.953
SIC leads to IPN	0.92	0.92	0.892	0.947
PDN leads to PCB	0.873	0.873	0.822	0.919
SIC leads to IKN	0.875	0.876	0.835	0.915
IKN leads to IPN	0.883	0.883	0.851	0.913
SIC leads to PCB	0.86	0.86	0.822	0.896
SI leads to OWN	0.839	0.839	0.791	0.886
OWN leads to PCB	0.829	0.829	0.771	0.881
IPN leads to OWN	0.836	0.836	0.791	0.878
IPN leads to PDN	0.814	0.814	0.761	0.864
IKN leads to PCB	0.805	0.806	0.752	0.856
SIC leads to PDN	0.788	0.789	0.725	0.849
IKN leads to OWN	0.788	0.788	0.732	0.843
PDN leads to OWN	0.739	0.74	0.663	0.812
IKN leads to PDN	0.686	0.687	0.62	0.751
PDN leads to PCC	0.145	0.162	0.082	0.267
PCC leads to PCB	0.101	0.135	0.078	0.224
IPN leads to PCC	0.134	0.161	0.124	0.209
IKN leads to PCC	0.073	0.107	0.064	0.173
PCC leads to OWN	0.074	0.105	0.062	0.166
SIC leads to PCC	0.079	0.104	0.066	0.154

Structural Model Testing

Structural testing of the model examines the relationship between the latent constructs in the model (Hair et al., 2019). The steps to examine the model were assessing structural model collinearity issues, explanatory power, predictive power, and the significance and relevance of the structural model relationship. To measure check for collinearity issues, Hair et al. (2019) recommended that the latent variable scores of the predictor constructs in partial regression are used to calculate the variance inflation factor (VIF) to ensure no collinearity that would otherwise bias the regression. They reported that established values are VIF <3 was used to ensure no collinearity, VIF > 5 suggested probable collinearity, and VIF greater than 10 suggested problematic collinearity.

VIF values were calculated for this study using SmartPLS 3 partial least squares algorithm. The VIF results of SmartPLS analysis are shown in Table 10. The VIF values for co-ownership perception were 2.02, salient social identity was 2.02, cost estimate in the privacy calculus was 1.637, and information privacy norms was 4.334. The privacy calculus benefit construct and the privacy decision construct showed a VIF value of 5.366 which was just above the fully acceptable value for collinearity. This collinearity was not unexpected since prior research shows correlation between benefits in the privacy calculus and beneficial privacy decisions (Krasnova & Veltri, 2010). As such the model may not be errant but just unable to fully assign the variance in each of constructs to either of the two variables (Hair et al., 2022). The measurement of the structural model showed VIF<3 for the rest of the constructs suggested no collinearity with PCB and PDN showed very low probability collinearity that was accepted. No or very low probability of collinearity meant the regression would not be biased.

Table 10

Collinearity Check – Variance Inflation Factor

	OWN	IPN	SIC	PCC	PCB	PDN
Intimate Knowledge (IKN)	1					
Co-Ownership Perception (OWN)		2.02	1	1	1	
Salient Social Identity (SIC)		2.02				
Benefit (PCB)						5.366
Cost (PCC)						1.637
Information Privacy Norms (IPN)						4.334

With low likelihood of collinearity in the structural model, the significance and relevance of the path coefficients was tested and is presented in the findings section. The coefficient of determination (R^2) for the endogenous constructs was then the next step in testing the structural model. R^2 has been reported to be a statistical measure of how much of the variance in the dependent variable is explained by the variation in the independent variables (Hair et al., 2019; Sekaran & Bougie, 2019). The variance of endogenous constructs which is the models explanatory power were examined using coefficient of determination (R^2) in SmartPLS 3 (Hair et al., 2019). According to Hair et al. (2019), for explanatory power testing $R^2 = 0.75$ was considered substantial, $R^2 = 0.50$ was considered moderate, $R^2 = 0.25$ was considered weak, and $R^2 >= 0.90$ indicated overfit. The results of the analysis of the endogenous constructs in the model show moderate explanatory power for co-ownership ($R^2 = 0.516$), salient social identity ($R^2 = 0.505$) and expected information privacy decisions ($R^2 = 0.639$). The model has substantial explanatory power

for the information privacy norm construct ($R^2 = 0.759$). A summary of the R^2 values is shown in Table 11.

Table 11

Explanatory Power – R Squared

	Construct	R^2
OWN	Co-Ownership Perception	0.516
PDN	Information Privacy Decision	0.639
IPN	Information Privacy Norms	0.759
SIC	Salient Social Identity	0.505

The models out-of-sample predictive power was tested next. The out-of-sample predictive power indicates the models ability to predict new or future observations (Hair et al., 2019). The partial least squares predict procedure in the PLS-SEM literature generates and evaluates predictions using training and holdout samples allowing a models predictive power to be tested (Shmueli et al., 2016). Shmueli et al.'s (2016) partial least squares predict procedure executes *k*-fold cross validation where the total dataset is randomly split into *k* equal subsets. Their procedure then uses all but one of the subsets as a training sample and uses the remaining subset to cross validate predicted value. By repeating this process *k* times, the models out of sample predictive statistics were calculated. Per Hair et al.'s (2019) recommendations, the focus was on our model's key endogenous construct of normative information privacy decisions not all endogenous constructs. The partial least squares predict procedure was run in SmartPLS with 10 folds, 10 repetitions, using the path weighting scheme, and 1000 iterations. The $Q^2_{predict}$ values for the PDN constructs (PDN1=0.35, PDN2=0.322) were greater than 0 indicating

that the indicator means from the analysis sample outperforms the naive benchmark as recommended (Hair et al., 2019). Table 12 shows the $Q^2_{predict}$ values for our endogenous construct of interest privacy decisions

Table 12

Predictive Power – Q^2 Predict

	Construct	$Q^2_{predict}$
PDN1	Privacy Decisions Norms (We-intentions 1)	0.35
PDN2	Privacy Decisions Norms (We-intentions 2)	0.322

Findings

Guidelines for how to use PLS-SEM recommended the final steps was to test statistical significance and relevance of the path coefficients using bootstrapping (Hair et al., 2019). Because PLS-SEM does not make any normality assumptions about the distribution of the data that was collected, parametric significance tests such as those used in regression analysis cannot be applied directly to check for significance of path-coefficients (Chin, 1998; Ringle et al., 2015). Ringle et al. (2015) detail that bootstrapping is the nonparametric procedure that allows tests for the statistical significance of PLS-SEM results such as path coefficients.

Path Significance and Relevance

SmartPLS was used for bootstrapping to see if the study's hypotheses were supported and were tested after study data was gathered (Hair et al., 2019). To conduct bootstrapping, a large number subsamples were repeatedly drawn from the original responses with replacement and used to estimate the partial least squares path model

(Davison & Hinkley, 1997; Efron & Tibshirani, 1993). 95% confidence intervals for significance testing were derived from the parameter estimates of the subsamples and the standard errors for the estimates are used to calculate *t*-values to assess the significance of each estimate (Hair et al., 2022; Ringle et al., 2015). Path coefficients statistical significance and relevance were tested using SmartPLS bootstrapping using 5000 samples. 0.05 significance, and a two tailed test consistent with Hair et al. (2019) recommendation. Path coefficients significance values were observed to lie between -1 and 1 indicating no error in the calculation. The coefficient's values were checked to be above the recommended critical *t*-value of 1.96 at the significance level of 5% for two tailed tests. SmartPLS was also used to test the moderation of the effect of cost and benefit components of the privacy calculus on the relationship between information privacy norms (IPN) and expected information privacy decisions as recommended in the literature (Sarstedt et al., 2020)

The relationships for each hypothesis were individually examined to ascertain that their path coefficients values were significantly different from zero allowing one to reject the null hypotheses that they had no effect. Table 13 shows the path co-efficient results including the original sample mean (β), the bootstrapped sample mean (M), standard deviation (STDEV), *t*-statistic, and *p*-values. The results addressed the problem of low intimate knowledge and low co-ownership perception of SMA among social media users lead to unexpected privacy decisions. The results for the nine hypotheses are discussed next.

The first hypothesis, H_1, tested whether SM users' level of intimate knowledge (IKN) of SMA generated from their SM content was positively correlated with their SMA co-

ownership perception. The results found that intimate knowledge has a significant positive impact on ownership perception in SMA (β=0.718, t=24.174, $p < 0.001$). Therefore H_1 was supported. Next H_2 tested if co-ownership perception (OWN) is positively correlated with the salient social identity (SIC) adopted in SMA information privacy decision making. The results found that co-ownership perception has a positive significant impact (β=0.705, t=27.577, $p < 0.001$) on the salient social identity adopted in SMA use. Therefore H_2 was supported. The third hypothesis, H_3, was set to test if salient social identity (SIC) adopted was positively correlated with the SMA information privacy norm (IPN) expected in SMA information privacy decision making. The results found that social identity had a significant positive impact (β=0.597, t=15.391, $p < 0.001$) on the information privacy norm. Therefore H_3 was supported.

The fourth hypothesis, H_4, was set to test if co-ownership perception (OWN) was positively corelated with the use of information privacy norms. The results found that co-ownership perception had a small positive and statistically significant impact on information privacy norms (β=0.34, t=8.202, $p < 0.001$). Therefore H_4 was supported. The fifth hypothesis, H_5, was set to test if co-ownership perception (OWN) was positively correlated with the benefit estimation in the privacy calculus. The results found that SMA co-ownership perception had a positive and significant impact on the benefit estimation in the privacy calculus (β=0.731, t=24.267, $p < 0.001$. Therefore H_5 was supported. The sixth hypothesis, H_6, set to test if co-ownership perception (OWN) is negatively correlated with the cost estimation in the privacy calculus for SMA information privacy use. The results found that co-ownership perception had a miniscule positive impact on ownership perception in SMA (β=0.064, t=0.757, $p = 0.225$).

However, its *t*-value of 0.757 did not exceed the critical value of 1.96. Therefore H_6 was not supported.

The seventh hypothesis, H_7, set to test if the benefit estimate in the privacy calculus had a moderating effect on the relationship between information privacy norms and information privacy decisions. The results found that benefit estimation had a significant negative moderating impact (β=-0.113, t=2.331, p = 0.01) on the relationship between information privacy norms and information privacy decisions in SMA. Therefore H_7 was supported. The next hypothesis, H_8, was tested to determine whether cost estimate in the privacy calculus moderated the positive relationship between the information privacy norms and SMA information privacy decisions. The results found the cost estimates moderating impact t-statistic to be at negative at -0.02, however its t-statistic was 0.477 which does not exceed the critical value of 1.96 for the 95% significance level (β=-0.02, t=0.477, p = 0.317). Therefore the null hypothesis was not rejected and H_8 was not supported. The ninth hypothesis, H_9, hypothesized that the adoption of SMA information privacy norms was positively correlated with normative information privacy decisions. The results found that information privacy norms had a significant positive impact (β=0.324, t=4.331, $p < 0.001$) on SMA information privacy decisions. Therefore H_9 was supported.

Table 13

Hypothesis Testing - Path Co-efficient

		Original Sample Mean (β)	**Sample Mean (*M*)**	**Standard Deviation (*STDEV*)**	***t*-Statistic (*t*)**	***p*-Value (*p*)**
H_1	Intimate Knowledge (IKN) leads to Co-Ownership Perception (OWN)	0.718	0.718	0.03	24.174	0.000
H_2	Co-Ownership Perception (OWN) leads to Salient Social Identity (SIC)	0.705	0.711	0.026	27.577	0.000
H_3	Salient Social Identity (SIC) leads to Information Privacy Norms (IPN)	0.597	0.595	0.039	15.391	0.000
H_4	Co-Ownership Perception (OWN) leads to Information Privacy Norms (IPN)	0.34	0.341	0.041	8.202	0.000
H_5	Co-Ownership Perception (OWN) leads to Benefit (PCB)	0.731	0.732	0.03	24.267	0.000
H_6	Co-Ownership Perception (OWN) leads to Cost (PCC)	0.064	0.068	0.085	0.757	0.225
H_7	Benefit moderating the IPN leads to Information Privacy Decision (PDN) relationship	-0.113	-0.113	0.049	2.331	0.01
H_8	Cost moderating the IPN leads to Information Privacy Decision (PDN) relationship.	-0.02	-0.014	0.042	0.477	0.317
H_9	Information Privacy Norms (IPN) leads to Information Privacy Decision (PDN)	0.324	0.329	0.075	4.331	0.000

Summary

The correlation value between variables in the hypothesized relationship was analyzed to confirm or disconfirm all the hypotheses at the commonly accepted social science research significance of $p = 0.05$ (Pavlou et al., 2007). Table 14 summarizes the results of hypothesis testing based on the PLS-SEM bootstrapping results. Seven of the nine hypotheses were supported while two were not. The supported relationships are discussed next.

Intimate knowledge was found to lead to co-ownership perception (H_1). Co-ownership perception was found to lead to salient social identity in SMA information privacy decision making (H_2). Evidence that salient social identity led to SMA information privacy norms (H_3) was found. Co-ownership perception was found to lead to normative information privacy use expectations (H_4). Additionally, co-ownership perception led to increase in the benefit estimate in the privacy calculus (H_5). The benefit estimate of the privacy calculus was found to negatively moderate the relationship between information privacy norms and information privacy decisions (H_7). Finally the impact of information privacy norms on expected information privacy decisions (H_9) was supported

The first unsupported relationship was between the co-ownership perception and costs estimation (H_6). The second unsupported relationship was on the moderating effect the cost-estimate in the privacy calculus on the relationship between the information privacy norm and the expected information privacy decision in SMA (H_8).

Table 14

Summary of Results

	Path	Result
H_1	Intimate Knowledge (IKN) leads to Co-Ownership Perception (OWN)	Supported
H_2	Co-Ownership Perception (OWN) leads to Salient Social Identity (SIC)	Supported
H_3	Salient Social Identity (SIC) leads to Information Privacy Norms (IPN)	Supported
H_4	Co-Ownership Perception (OWN) leads to Information Privacy Norms (IPN)	Supported
H_5	Co-Ownership Perception (OWN) leads to Benefit (PCB)	Supported
H_6	Co-Ownership Perception (OWN) leads to Cost (PCC)	Not supported
H_7	Benefit Moderating IPN to IPD leads to Information Privacy Decision (PDN)	Supported
H_8	Cost Moderating IPN to IPD leads to Information Privacy Decision (PDN)	Not supported
H_9	Information Privacy Norms (IPN) leads to Information Privacy Decision (PDN)	Supported

Chapter 5

Conclusions

Overview

The primary purpose of this research was to examine theory and a model that can be used to understand the relationship between intimate knowledge and co-ownership of SMA on social identity, information privacy norms, and the information privacy calculus in a bid to reduce counter normative SMA information privacy decisions. To do so theory extension, a model, and various hypotheses were developed. A research methodology was defined, data collected using a measurement instrument, and the resulting data analyzed. The results were examined, interpreted, and inferences were drawn from them. The four sections below: conclusions, implications, recommendation, and summary conclude this chapter.

First, in the conclusion section, each hypothesis is discussed considering the analysis of the results and previous research. In addition, the underlying theory development and previous studies was be examined for congruence with existing literature. Conclusions about the results strengths, weaknesses and limitations are discussed. Secondly, in the implications section, the impact of the study on the field, contributions to knowledge, and potential contributions to professional practice are highlighted. Third, recommendations for future research, theoretical concepts, and organizational practice are presented. Finally, the report concludes with a summary of the whole study.

Conclusions

Social media analytics is important to many businesses for their operations. This type of knowledge is derived from social media data after some privacy allowance for use

have been made by those businesses' users. However, businesses functions risk major disruption when SMA information privacy use is perceived to run afoul of user expectations. Prior IS literature had theorized on how users could be better involved in the SMA information privacy decision making process with limited empirical evidence. The theory of multilevel information privacy outlined the constructs that would contribute to joint and normative information privacy management between companies and users. TMIP examined co-ownership perception as the starting point for co-ownership and subsequent normative decision making. However, because companies had previously held most SMA in secret, levels of co-ownership perception measurement remained under explored. To measure SMA co-ownership levels, the intimate knowledge construct from the theory of psychological ownership in organization was added as a precursor to co-ownership perception in TMIP. A combined theory based model was developed, an instrument developed, data collected and analyzed to address the research problem. The research problem that was empirically examined in this study was low levels of intimate knowledge and co-ownership led to non-normative salient social identities, information privacy rules, and cost-benefit estimations in the privacy calculus which led to unexpected information privacy decisions (Bélanger & James, 2020).

Analysis of the study results showed that there was a strong positive correlation between SMA intimate knowledge and co-ownership perception supporting hypothesis 1. The result validated the addition of the intimate knowledge component to TMIP's theory for this study. It empirically measured the intimate knowledge concept from the psychological ownership literature (Bélanger & James, 2020; Kwon, 2020; Pierce et al., 2001). This result was consistent with existing studies that demonstrate a positive

correlation between intimate knowledge and ownership perception in information privacy decision making (Giordano et al., 2020; Kwon, 2020). The results are consistent with Giordano et al.'s (2020) study that showed that intimate knowledge of work products in teams lead to co-ownership perceptions. Kwon (2020) similarly empirically showed more specifically that users ownership perceptions toward social media data was positively correlated with their participation in social media. One could argue that information privacy decision making for SMA is both a form of a team or group product from social media. This study empirically demonstrated that for SMA intimate knowledge is the beginning of co-ownership perception.

The results showed a strong positive relationship between co-ownership perception and the social identity assumed for the privacy decision supporting hypothesis 2. Calls for more group information privacy studies had been a reoccurring theme in the information privacy literature generally (Bélanger & Crossler, 2011; Smith et al., 2011). Recent study presented the theoretical foundation for the relationship between group ownership and the social identity in privacy decision making (Bélanger & James, 2020). Bélanger and James (2020) call for researchers to examine whether a personal or salient social identity is active. The strong correlation between co-ownership and salient social identity in this study answered this call and was consistent with prior studies (Algesheimer et al., 2005; Gabisch & Milne, 2014; Hong & Thong, 2013; Sharma & Crossler, 2014). The result was consistent with Algesheimer et al. (2005) early marketing literature study that showed that the European car club users formed a joint social identity once users had co-ownership perception over the car brand. This result was also in line with both the Gabisch and Milne (2014) and Sharma and Crossler (2014) studies that demonstrated that

user developed joint social identities with enterprises over co-owned knowledge. Finally, the result aligned with Hong and Thong's (2013) study that showed that group aligned social units when privacy decisions are being made over shared data.

Hypothesis 3 was supported by the results that show a positive correlation between salient social identity and the information privacy norm expectation. The theoretical foundation for this relationship is provided from communication social identity theory and self-categorization theory and by TMIP in the IS literature (Bélanger & James, 2020; Ellemers & Haslam, 2012; Reynolds, 2017). This result added to previous empirical study that validated the impact of salient social identity on information privacy rules use expectation (Tsai & Bagozzi, 2014). Like Tsai and Bagozzi's (2014) study in virtual communities, the fourth hypothesis' result empirically demonstrated that social identities correspond to group social norm expectations.

The results also supported hypothesis 4 by showing that SMA co-ownership perception has a strong positive correlation with the information privacy norms adopted for the privacy decision making. This was consistent with existing literature that has shown that ownership perception was an antecedent of information privacy norms (Zhu & Kanjanamekanant, 2020). This result was consistent with Zhu and Kanjanamekanant's (2020) ad privacy study held that co-ownership perception led Facebook users to expect normative privacy rules. Similar, co-ownership perception in this study had a strong positive correlation with information privacy rule expectation. The result was also theoretically consistent with the relationship posited in the communications privacy literature and specifically in IS by the theory of multilevel information privacy (Bélanger & James, 2020; Petronio, 2002).

Hypothesis 5 was supported by the results that showed that co-ownership perception was positively correlated to the benefit estimate in the privacy calculus. The TMIP provided the theoretical underpinnings suggesting that the benefit estimate was affected by co-ownership perception and calls for its study (Bélanger & James, 2020). This result was consistent with previous studies had shown an increase in ownership perception was positively correlated to benefit estimate in the privacy calculus (Cichy et al., 2014; Gabisch & Milne, 2014; Sharma & Crossler, 2014). Previous studies showed that relinquishing an individual right to data ownership increased disclosure decisions for some benefit estimation. The strong positive correlation between co-ownership perception and the benefit estimate in the privacy calculus is consistent with these prior results.

The relationship between co-ownership perception and cost in the privacy calculus was not significant and therefore hypothesis 6 was not supported. The TMIP presents that the theoretical basis that co-ownership perception would impact the cost-benefit estimate without parsing whether costs or benefits would be significant (Bélanger & James, 2020). Bélanger and James (2020) left the question of whether costs in the privacy calculus were affected by group ownership as a future research question. There wasn't sufficient significance in the data set to support hypothesis 6. The IS literature may provide possible explanations for why co-ownership had an insignificant impact on cost in the privacy calculus. Users had been shown to exhibit several attitudes that minimize cost estimation in the privacy calculus in SMA. Prior research in other contexts had shown attitudes that contribute to costs minimization including an online privacy optimism bias, overconfidence once given some control, and underestimation of privacy cost when

presented with a positive outcome among others (Baek et al., 2014; Brandimarte et al., 2013). Similarly, the results of our study show very low original sample means for the path coefficients that involve cost estimation in the privacy calculus. The relationship between co-ownership perception and cost estimation in the privacy calculus (H_6) has an original sample mean of 0.064. It is likely that benefit minimization may be occurring due to the novelty or other characteristic inherent in SMA contexts.

Hypothesis 7 was supported by the result that shows that the benefit estimate in the privacy calculus moderated the positive relationship between information privacy norms and normative information privacy decisions in such a way that when the benefits estimate was low, it weakened the positive relationship. This result is consistent with prior results in the social media context that showed that high benefits estimates led to high intentions to make normative information privacy decisions from normative rules (Krasnova & Veltri, 2010). Krasnova and Veltri's (2010) study showed that USA Facebook users estimated higher benefits from its use and therefore disclosed more on the SNS. The result in the seventh hypothesis affirms this assertion for SMA in the same cultural context.

The moderating effect of cost in the privacy calculus on the positive relationship between information privacy norms and information privacy decisions were insignificant meaning hypothesis 8 was not supported. The TMIP presented that the theoretical basis that the cost-benefit estimate could possibly have an impact on the relationship between IPNs and PDNs (Bélanger & James, 2020). Bélanger and James (2020) left the question of whether costs in the privacy calculus were affected by group ownership as a future research question. There wasn't sufficient significance in the data set to reject the null

hypothesis. As such hypothesis 8 was not supported. The moderating effect of cost estimation in the privacy calculus on the relationship (H_8) between information privacy norms and normative information privacy expectation is -0.02. Similar to hypothesis 6 this result may be explained by prior research that a multitude of factors minimize the cost estimation in the SMA privacy calculus namely online privacy optimism bias, overconfidence once given some control, and underestimation of privacy cost when presented with a positive outcome among others (Baek et al., 2014; Brandimarte et al., 2013).

Hypothesis 9 was supported by the results that show that information privacy norms were positively correlated with information privacy decisions. The TMIP provided the theoretical underpinnings that suggested that IPNs that were normative to the stimulated salient social identity were typically used to make the privacy decision unless the cost estimate was too high relative to the benefit estimate in the privacy calculus (Bélanger & James, 2020). Bélanger and James (2020), hypothesized that users expected more normative MIPDs would be made when the more normative IPN were selected. This result was consistent with previous studies which showed that normative IPNs were positively correlated to normative privacy decisions (Krasnova & Veltri, 2010). Krasnova and Veltri's (2014) study showed that privacy norms in societies affected whether Facebook uses expected a normative information privacy decision. This study validates that finding using a different type of group, the joint users and enterprise group, in managing information privacy decision making in the SMA context.

The study had several strengths, weaknesses, and limitations tied to the sample, data collection methods, measurement and analysis. The strength of the study was its use of

validated measures for all items in the construct with only minimal word changes. This ensured that the constructs being measured had previously been validated and were commonly accepted for use in studies of this kind. For limitations, this study sample was obtained exclusively from participants in the USA who had were on the Amazon Turk service. While previous research has shown that Amazon Turk produced a varied sample (Lowry et al., 2016; Mason & Suri, 2012), future research could verify that the results obtained here are not limited to USA by widening the sample to users outside the United States. A potential weakness present was that there were few validated items to measure the salient social identity construct and the intimate knowledge construct. Future study could be strengthened by validating a more robust survey instrument for these two constructs.

Implications

Several theoretical and managerial implication arise from this study. The theoretical contributions include in information privacy theory development, nascent study in SMA information privacy, and novel group information study. The practice implications are drawn from user insights for SMA. They include implications for increasing user SMA intimate knowledge, information privacy norms, and preventing counter normative decisions.

Theoretical Implications

This study contributes to theory development by adding and validating the intimate knowledge construct from psychological ownership theory in organizations as the conceptual antecedent to co-ownership perception to TMIP (Bélanger & Crossler, 2019; Petronio, 2002). Bélanger and James (2020) raise data analytics and socialization context

as a useful and rich area for subsequent research work to validate TMIP. However, for data analytics, lack of knowledge was an acknowledged information privacy threat that could lead to confounding results if TMIP constructs alone were utilized (Yun et al., 2019). As such this study, contributes by combining adding and validating the intimate knowledge construct from PO theory to the TMIP.

Examining the role of intimate knowledge of an understudied information type: SMA contributed to the literature. This contribution was especially important because of its joint ownership was widely acknowledged to be under examined in various contexts but was a root cause of negative affectations when SMA information privacy violations were perceived to have occurred (Acquisti et al., 2015; Bélanger & James, 2020; Holsapple et al., 2018).

The intimate knowledge construct from psychological ownership (PO) theory had previously been studied in social media at the group level that consists of multiple users but not much at as a multilevel concept that examined group co-ownership whose members were SM users and the SM service provider (Zhu & Kanjanamekanant, 2020). This study contributes to the information privacy literature by examining a novel domain combination to the SMA literature group composition: user and company jointly. This group composition which was explored in other social sciences such as marketing but not as much in IS, had long been remarked upon but was empirically under studied in the information privacy literature (Algesheimer et al., 2005).

Practical Implications

The practical implications include suggestions for managing SMA intimate knowledge, co-ownership perception, social identities and information privacy norms. These are

offered in the hopes of reducing negative business affectations from perceived information privacy violations. Practitioners are encouraged to develop practices that increase SMA intimate knowledge among social media users rather hiding SMA content. While businesses often held SMA close for competitive advantage, this study showed that intimate knowledge of SMA among users was strongly correlated with expected privacy decisions. As such, it's much more likely that user affectations that lead to revolts, government regulation, and threaten firm existence would occur if SM users had intimate knowledge of SMA.

Co-ownership perception was shown to have a strong correlation with the perception that SMA privacy decisions were congruent with user expectation. Companies should work on mechanism to increased co-ownership in line with the results of this study and previous study that encourage such approaches (Zhu & Kanjanamekanant, 2020). This can be done by encouraging two-way firm-user discourse with representatives of the firm around the SMA held and its use. Strategies from the marketing literature such as regional brand ambassadors and evangelists from firms to their users and popularly chosen user representatives to the firms can be adopted in SM to reinforce co-ownership (Algesheimer et al., 2005).

Salient social identity and information privacy norms were both positively correlated with SMA privacy decision making. As such, common social identities should and privacy norms for SMA should be developed and jointly shared between firms and users. Finally, the benefit estimate in the privacy calculus was positively correlated with normative information privacy decisions. While developing co-owned mechanisms for privacy decision making, firms should highlight the benefits of privacy decisions that are

made using agreed upon information privacy norms. This is likely to increase customer information privacy management satisfaction.

Recommendations

This study's limitations give rise to various potential future areas of study. The TMIP presents "online only" and "online and offline" environmental characteristics that may have an impact on multilevel information privacy management (Bélanger & James, 2020). This study was limited to online only characteristics of SMA with the firm being a virtual person in the group rather than a physical privacy officer of the firm. Future research could examine both online and offline environment characteristics such as physical firm representatives, physical locations like privacy conferences, and the format of the SMA used such as video, audio. In addition, this study evaluated SMA privacy at a given point in time. Qualitative feedback from this study revealed that many participants were only beginning to think about SMA information privacy as they were presented with study questions related to their joint privacy management role with SM firms. Future studies can examine the evolution of user multilevel privacy management constructs over time. Such studies would contribute to a more robust view of users' expectations and further reduce negative affectations and related business disruptions.

Summary

The goal of this study was to examine the impact of levels of SMA intimate knowledge and co-ownership perception on users SMA privacy decision expectations. The theory of multilevel information privacy (TMIP) and the theory for psychological ownership in organizations (PO) were used to develop a model and several hypotheses.

The study's objective of reducing counter normative SMA privacy decisions faced the initial hurdle that if companies hold SMA as close a closely guarded secret SM users would only contribute when impactful counter normative privacy decision had been made (Bélanger & Crossler, 2019; Holsapple et al., 2018). The emergence of publicly accessible SMA was used in this study to confirm that intimate knowledge has a strong correlation with co-ownership perception which TMIP held was a precursor to privacy management involvement. As such the objective of reducing unexpected SMA privacy decision begins with examining user's SMA intimate knowledge.

In addition, the salient social identity, benefit estimate in the privacy calculus, and information privacy norms were positively correlated with a normative privacy decision expectation. As expected, the salient social identity was positively correlated with the information privacy norm the user expected for co-owned SMA. This empirically confirms TMIP's theorizing that suggests each contributes to expected information privacy decisions in the SMA context (Bélanger & James, 2020). For this study, the correlations between co-ownership and the cost estimate in the privacy calculus and the cost estimate's moderating role on the relationship between IPNs and PDNs were not statistically significant as expected.

Appendix A

Questionnaire

Hello,

Thank you for filling out this questionnaire. Doing so will help Bradley A Wangia, a doctoral student at Nova Southeastern University College of Computing and Engineering, better understand your analytics information privacy management preferences on Facebook. Answering the questions in a forthright manner and to the best of your ability will benefit future researchers and companies seeking to develop privacy management practices that are more to social media users' liking. Your identity will be kept anonymous throughout, and the survey should not take more than 30 minutes to complete. A summary of the aggregated results of the study and its conclusions will be available for your review once the study is complete.

Thank you

Bradley A Wangia

NSU Florida
NOVA SOUTHEASTERN UNIVERSITY

INSTITUTIONAL REVIEW BOARD
3301 College Avenue
Fort Lauderdale, Florida 33314-7796
PHONE: (954) 262-5369

Participant Letter for Anonymous Surveys
NSU Consent to be in a Research Study Entitled
Social Media Analytics Information Privacy Decisions: Impact of User Intimate Knowledge and Co-ownership Perceptions

Who is doing this research study?

This person doing this study is Bradley A. Wangiax with College of Computing and Engineering. They will be helped by Ling Wang, PhD/Dissertation Chair

Why are you asking me to be in this research study?

You are being asked to take part in this research study because you are volunteered as an adult social media user in the United States of American and you can help examine social media analytics privacy management practices.

Why is this research being done?

The purpose of this study is to find out whether the level of intimate knowledge of social media analytics and co-ownership perception among social media users impacts their expectation to be involved in its privacy management.

What will I be doing if I agree to be in this research study?

You will be taking a one-time, anonymous survey. The survey will take approximately 30 minutes to complete.

Are there possible risks and discomforts to me?

This research study involves minimal risk to you. To the best of our knowledge, the things you will be doing have no more risk of harm than you would have in everyday life.

What happens if I do not want to be in this research study?

You can decide not to participate in this research and it will not be held against you. You can exit the survey at any time.

Will it cost me anything? Will I get paid for being in the study?

There is no cost for participation in this study. Participation is voluntary and you will be given a $0.30 Amazon MTurk payment for completing the questionnaire in this research study.

How will you keep my information private?

Your responses are anonymous. Information we learn about you in this research study will be handled in a confidential manner, within the limits of the law. Your information under US data privacy laws. This

NSU Florida
NOVA SOUTHEASTERN UNIVERSITY

INSTITUTIONAL REVIEW BOARD
3301 College Avenue
Fort Lauderdale, Florida 33314-7796
PHONE: (954) 262-5369

data will be available to the researcher, the Institutional Review Board and other representatives of this institution, and any granting agencies (if applicable). If we publish the results of the study in a scientific journal or book, we will not identify you. All confidential data will be kept securely in encrypted storage within the system. All data will be kept for 36 months from the end of the study and destroyed after that time by permanent deletion from the system.

Who can I talk to about the study?

If you have questions, you can contact the primary researcher Bradley A Wangia at 267-702-3450. Dr. Ling Wang can be reached at lingwang@nova.edu

If you have questions about the study but want to talk to someone else who is not a part of the study, you can call the Nova Southeastern University Institutional Review Board (IRB) at (954) 262-5369 or toll free at 1-866-499-0790 or email at IRB@nova.edu.

Do you understand and do you want to be in the study?

If you have read the above information and voluntarily wish to participate in this research study, please click on the link below to access the survey.

Click Here to Access Survey

Questions

Based on a scale of 1 to 5, with 1 indicating that you strongly disagree with the and 5 indicating that you strongly agree with the statement presented, circle the number that matches your response. The first question is only an example.

Facebook uses a variety of data sources to determine which advertisements are interesting and useful to you when you log into Facebook.

Example Question: I know the sources of the data used to determine which advertisements I am shown on Facebook.

1	2	3	4	5
Strongly Disagree	Disagree	Undecided	Agree	Strongly Agree

Introduction

The first few questions will ask for your level of familiarity with social media analytics. The rest of the survey will ask you about the social media analytics depending on your responses.

1. Regarding this Facebook social connectedness index analytics, I am

1	2	3	4	5
Very Unfamiliar	Somewhat Familiar	Neither Familiar nor Unfamiliar	Somewhat familiar	Very familiar

2. Regarding this Facebook movement range maps analytics, I am

1	2	3	4	5
Very Unfamiliar	Somewhat Familiar	Neither Familiar nor Unfamiliar	Somewhat familiar	Very familiar

3. Regarding this Facebook COVID 19 forecasts analytics, I am

1	2	3	4	5
Very Unfamiliar	Somewhat Familiar	Neither Familiar nor Unfamiliar	Somewhat familiar	Very familiar

4. Regarding this Facebook travel patterns analytics, I am

1	2	3	4	5
Very Unfamiliar	Somewhat Familiar	Neither Familiar nor Unfamiliar	Somewhat familiar	Very familiar

5. Regarding this Facebook relative wealth index analytics, I am

1	2	3	4	5
Very Unfamiliar	Somewhat Familiar	Neither Familiar nor Unfamiliar	Somewhat familiar	Very familiar

6. Please enter any other social media analytics that you are familiar with.

Facebook Social Connectedness Index (SCI) is used for the questions in the rest of this survey assuming that it was the most familiar SMA type. If another SMA was chosen, the respondent will be asked about that SMA. The most familiar SMA from the pilot study will be used for all respondents in the actual study.

7. Regarding the services offered from Facebook Social Connectedness Index, are you

1	2	3	4	5	6	7
Unfamiliar			Moderately Familiar			Familiar

8. Regarding the services offered from Facebook Social Connectedness Index, are you

1	2	3	4	5	6	7
Inexperienced			Moderately Experienced			Extremely Experienced

9. Regarding the services offered from Facebook Social Connectedness Index, are you

1	2	3	4	5	6	7
Not Knowledgeable			Moderately Knowledgeable			Extremely Knowledgeable

10. I feel Facebook has the right to use the Social Connectedness Index.

1	2	3	4	5
Strongly Disagree	Disagree	Undecided	Agree	Strongly Agree

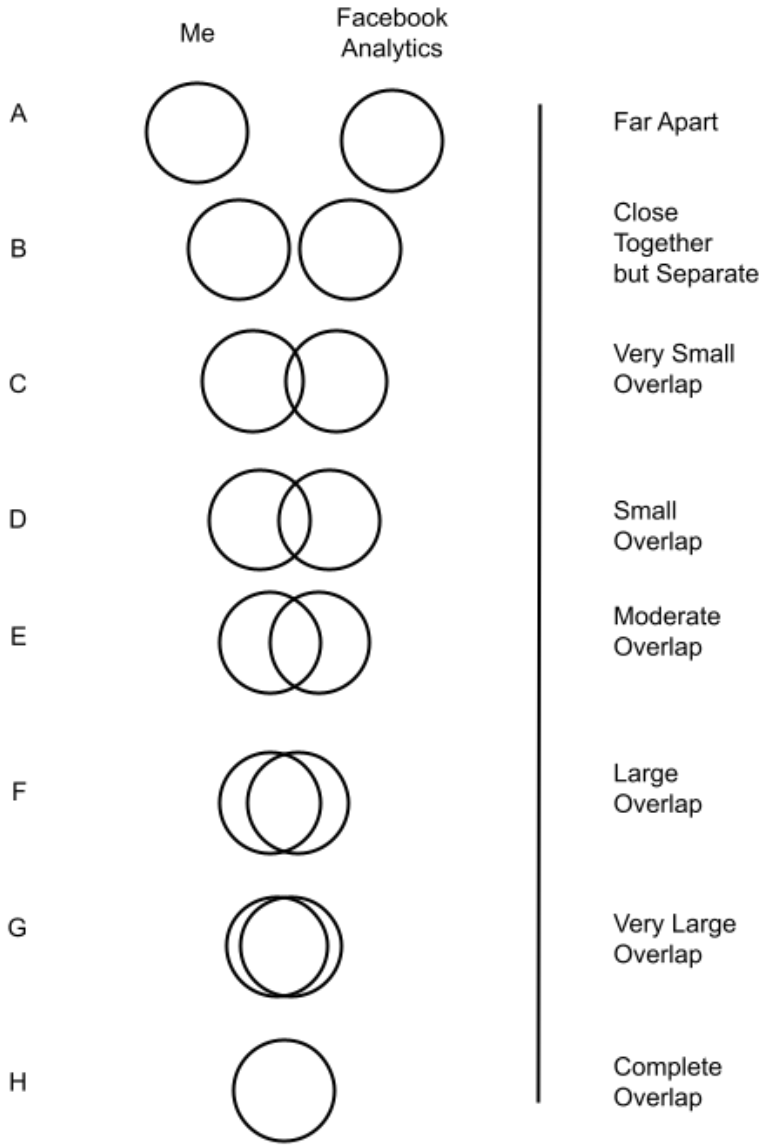
11. I feel the Social Connectedness Index belongs to Facebook too.

1	2	3	4	5
Strongly Disagree	Disagree	Undecided	Agree	Strongly Agree

12. I feel Facebook and I co-own the Social Connectedness Index.

1	2	3	4	5
Strongly Disagree	Disagree	Undecided	Agree	Strongly Agree

13. How would you express the degree of overlap between your personal identity and the identity of a joint (Facebook and you) group formed to manage Social Connectedness Index privacy decisions?



14. Please indicate to what degree your self-image overlaps with the identity of the joint group as you perceive it.

1	2	3	4	5	6	7
Not at all			moderately			Very much

15. When I face challenges in my life, I feel comfortable talking about them on my Facebook account used to create the Social Connectedness Index.

1	2	3	4	5	6	7
Not at all			moderately			Very much

16. I like my Facebook entries to be long and detailed on the Facebook account that is used to create SCI analytics.

1	2	3	4	5	6	7
Not at all			moderately			Very much

17. I like to discuss work concerns on my Facebook account that is used to create SCI analytics.

1	2	3	4	5	6	7
Not at all			moderately			Very much

18. I often tell intimate, personal things on my Facebook account that is used to create SCI analytics without hesitation.

1	2	3	4	5	6	7
Not at all			moderately			Very much

19. I share information with people whom I don't know in my day-to-day life.

1	2	3	4	5	6	7
Not at all			moderately			Very much

20. I update my Facebook account that is used to create SCI analytics frequently.

1	2	3	4	5	6	7
Not at all			moderately			Very much

21. I have limited personal information on my Facebook account that is used to create SCI analytics.

1	2	3	4	5	6	7
Not at all			moderately			Very much

22. I use shorthand (e.g. pseudonyms or limited details) when discussing sensitive information on my Facebook account that is used to create SCI analytics.

1	2	3	4	5	6	7
Not at all			moderately			Very much

23. If I think that the information I posted on my Facebook account that is used to create SCI analytics really looks too private, I might delete it.

1	2	3	4	5	6	7
Not at all			moderately			Very much

24. I usually am slow to talk about recent events on my Facebook account that is used to create SCI analytics because people might talk.

1	2	3	4	5	6	7
Not at all			moderately			Very much

25. I don't post on my Facebook account used to create Facebook social connectivity index analytics about certain topics because I worry about who has access.

1	2	3	4	5	6	7
Not at all			moderately			Very much

26. Seeing intimate details about someone else through my Facebook account that is used to create SCI analytics makes me feel I should take steps to keep their information private.

1	2	3	4	5	6	7
Not at all			moderately			Very much

27. I accurately update the profile on my Facebook account that is used to create SCI analytics so others can find me.

1	2	3	4	5	6	7
Not at all			moderately			Very much

28. I try to let people know my best interests on my Facebook account that is used to create SCI analytics so we can be friends.

1	2	3	4	5	6	7
Not at all			moderately			Very much

29. I allow people with a profile that I don't know to have access to my Facebook account that is used to create SCI analytics.

1	2	3	4	5	6	7
Not at all			moderately			Very much

30. I comment on others Facebook posts to have others check out my Facebook account that is used to create SCI analytics.

1	2	3	4	5	6	7
Not at all			moderately			Very much

31. I allow anonymous access to my Facebook account that is used to create SCI analytics.

1 2 3 4 5 6 7
Not at all moderately Very much

32. I regularly make friend requests to interesting profiles to increase traffic to the Facebook account that is used to create SCI analytics.

1 2 3 4 5 6 7
Not at all moderately Very much

33. In general, it would be risky to disclose personal information on my Facebook account that is used to create SCI analytics.

1 2 3 4 5 6 7
Not at all moderately Very much

34. There would be high potential for privacy loss associated with giving my personal information on my Facebook account that is used to create SCI analytics.

1 2 3 4 5 6 7
Not at all moderately Very much

35. Personal information on my Facebook account that is used to create SCI analytics could be inappropriately used.

1 2 3 4 5 6 7
Not at all moderately Very much

36. Providing personal information on my Facebook account that is used to create SCI analytics would involve many unexpected problems.

1 2 3 4 5 6 7
Not at all moderately Very much

37. Revealing personal information on my Facebook account that is used to create SCI analytics will help me obtain information/products/services I want.

1 2 3 4 5 6 7
Not at all moderately Very much

38. I need to provide my personal information on my Facebook account that is used to create SCI analytics so I can get what I want from Facebook.

1 2 3 4 5 6 7

Not at all moderately Very much

39. I believe that as a result of my personal information disclosure on my Facebook account that is used to create SCI analytics, I will benefit from a better, customized service and or better information and products.

1	2	3	4	5	6	7
Not at all			moderately			Very much

40. I intend that the group [i.e. Facebook and I identified as a group prior] manage the privacy of the analytics generated from my Facebook account in the next.

1	2	3	4	5
Strongly Disagree	Disagree	Undecided	Agree	Strongly Agree

41. We [i.e. Facebook and I identified as a group prior] will jointly manage the privacy of the analytics generated from personal information from my Facebook account.

1	2	3	4	5
Strongly Disagree	Disagree	Undecided	Agree	Strongly Agree

42. How old are you?

- ○ Under 18 (1)
- ○ 18-24 years old (2)
- ○ 25-34 years old (3)
- ○ 35-44 years old (4)
- ○ 45-54 years old (5)
- ○ 55-64 years old (6)
- ○ 65+ years old (7)

43. How do you describe yourself?

- ○ Male (1)
- ○ Female (2)
- ○ Non-binary / third gender (3)
- ○ Prefer to self-describe (4)

_____

- ○ Prefer not to say (5)

44. Choose one or more races that you consider yourself to be:

- ☐ White (1)
- ☐ Black or African American (2)
- ☐ American Indian or Alaska Native (3)
- ☐ Asian (4)
- ☐ Hispanic (5)
- ☐ Native Hawaiian or Pacific Islander (6)
- ☐ Other (7) _____

45. What is the highest level of school you have completed or the highest degree you have received?

- ○ Less than high school degree (1)
- ○ High school graduate (high school diploma or equivalent including GED) (2)
- ○ Some college but no degree (3)
- ○ Associate degree in college (2-year) (4)
- ○ Bachelor's degree in college (4-year) (5)
- ○ Master's degree (6)
- ○ Doctoral degree (7)
- ○ Professional degree (JD, MD) (8)

46. In which state do you currently reside?

▼ Alabama (1) ... I do not reside in the United States (53)

47. Please indicate the answer that includes your entire household income in (previous year) before taxes.

- ○ Less than $10,000 (1)
- ○ $10,000 to $19,999 (2)
- ○ $20,000 to $29,999 (3)
- ○ $30,000 to $39,999 (4)
- ○ $40,000 to $49,999 (5)
- ○ $50,000 to $59,999 (6)
- ○ $60,000 to $69,999 (7)
- ○ $70,000 to $79,999 (8)
- ○ $80,000 to $89,999 (9)
- ○ $90,000 to $99,999 (10)
- ○ $100,000 to $149,999 (11)
- ○ $150,000 or more (12)

48. Which social media site do you use most often?

- ○ Facebook (1)
- ○ Instagram (2)
- ○ Twitter (3)

○ Other (4) _____

49. How often do you use Facebook?

○ Never (1)

○ Once a year (8)

○ Once a month (9)

○ Once a week (2)

○ 2-3 times a week (3)

○ 4-6 times a week (4)

○ Once a day (5)

○ 2-3 times a day (6)

○ more than 5 times a day (7)

50. Please enter any feedback

_____

Appendix B

Institutional Review Board Approval Memo

NOVA SOUTHEASTERN UNIVERSITY
Institutional Review Board

MEMORANDUM

To: Bradley Wangia, M.Sc
College of Engineering and Computing

From: Ling Wang, Ph.D.
College Representative, College of Engineering and Computing

Date: December 30, 2021

Subject: IRB Exempt Initial Approval Memo

TITLE: Social Media Analytics Information Privacy Decisions: Impact of User Intimate Knowledge and Co-ownership Perceptions– NSU IRB Protocol Number 2021-624

Dear Principal Investigator,

Your submission has been reviewed and Exempted by your IRB College Representative or their Alternate on **December 30, 2021**. You may proceed with your study.

Please Note: Exempt studies do not require approval stamped documents. If your study site requires stamped copies of consent forms, recruiting materials, etc., contact the IRB Office.

Level of Review: Exempt

Type of Approval: Initial Approval

Exempt Review Category: Exempt 2: Interviews, surveys, focus groups, observations of public behavior, and other similar methodologies

Post-Approval Monitoring: The IRB Office conducts post-approval review and monitoring of all studies involving human participants under the purview of the NSU IRB. The Post-Approval Monitor may randomly select any active study for a Not-for-Cause Evaluation.

Annual Status of Research Update: You are required to notify the IRB Office annually if your

3301 College Avenue • Fort Lauderdale, Florida 33314-7796
(954) 262-5369 • 866-499-0790 • Fax: (954) 262-3977 • Email: *irb@nova.edu* • Web site: *www.nova.edu/irb*

research study is still ongoing via the *Exempt Research Status Update xForm.*

Final Report: You are required to notify the IRB Office within 30 days of the conclusion of the research that the study has ended using the *Exempt Research Status Update xForm*.

Translated Documents: No

Please retain this document in your IRB correspondence file.

CC: Ling Wang, Ph.D.

Ling Wang, Ph.D.

References

Acar, A., Aksu, H., Uluagac, A. S., & Conti, M. (2018). A survey on homomorphic encryption schemes: Theory and implementation. *ACM Computing Surveys*, *51*(4), 1–35. https://doi.org/10.1145/3214303

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–514. https://doi.org/10.1126/science.aaa1465

Aguirre-Urreta, M. I., & Rönkkö, M. (2018). Statistical inference with PLSc using bootstrap confidence intervals. *MIS Quarterly*, *42*(3), 1001–1020. https://doi.org/10.25300/MISQ/2018/13587

Alashoor, T., Han, S., & Joseph, R. C. (2017). Familiarity with big data, privacy concerns, and self-disclosure accuracy in social networking websites: An APCO model. *Communications of the Association for Information Systems*, *41*, 62–96. https://doi.org/10.17705/1CAIS.04104

Algesheimer, R., Dholakia, U. M., & Herrmann, A. (2005). The social influence of brand community: Evidence from European car clubs. *Journal of Marketing*, *69*(3), 19–34. https://doi.org/10.1509/jmkg.69.3.19.66363

Altman, Irwing. (1975). *The environment and social behavior: Privacy, personal space, territory, and crowding.* Brooks/Cole Publishing Company.

Auxier, B., & Anderson, M. (2021, April 7). *Social media use in 2021*. Pew Research Center. https://www.pewresearch.org/internet/2021/04/07/social-media-use-in-2021/

Baek, Y. M., Kim, E., & Bae, Y. (2014). My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns. *Computers in Human Behavior*, *31*, 48–56. https://doi.org/10.1016/j.chb.2013.10.010

Bagozzi, R. P., & Lee, K.-H. (2002). Multiple routes for social influence: The role of compliance, internalization, and social identity. *Social Psychology Quarterly*, *65*(3), 226. https://doi.org/10.2307/3090121

Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science*, *16*(1), 74–94. https://doi.org/10.1007/BF02723327

Barth-Jones, D. C. (2012). The "re-identification" of Governor William Weld's medical information: A critical re-examination of health data identification risks and privacy protections, then and now. *Social Sciences Research Network*, *1*(1), 19. https://doi.org/10.2139/ssrn.2076397

Beaglehole, E. (1932). *Property: A study in social psychology*. Macmillan.

Bélanger & Crossler. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, *35*(4), 1017. https://doi.org/10.2307/41409971

Bélanger, F., & Crossler, R. E. (2019). Dealing with digital traces: Understanding protective behaviors on mobile devices. *The Journal of Strategic Information Systems*, *28*(1), 34–49. https://doi.org/10.1016/j.jsis.2018.11.002

Bélanger, F., & James, T. L. (2020). A theory of multilevel information privacy management for the digital era. *Information Systems Research*, *31*(2), 510–536. https://doi.org/10.1287/isre.2019.0900

Bélanger, F., & Xu, H. (2015). The role of information systems research in shaping the future of information privacy: Editorial. *Information Systems Journal*, *25*(6), 573–578. https://doi.org/10.1111/isj.12092

Bergami, M., & Bagozzi, R. P. (2000). Self-categorization, affective commitment and group self-esteem as distinct aspects of social identity in the organization. *British Journal of Social Psychology*, *39*(4), 555–577. https://doi.org/10.1348/014466600164633

Blocki, J., Blum, A., Datta, A., & Sheffet, O. (2013). Differentially private data analysis of social networks via restricted sensitivity. *Proceedings of the 4th Conference on Innovations in Theoretical Computer Science - ITCS '13*, 87. https://doi.org/10.1145/2422436.2422449

Bost, R., Popa, R. A., Tu, S., & Goldwasser, S. (2015). Machine learning classification over encrypted data. *Proceedings of the 2015 Network and Distributed System Security Symposium*, 220–234. https://doi.org/10.14722/ndss.2015.23241

Bradlow, E. T., Gangwar, M., Kopalle, P., & Voleti, S. (2017). The role of big data and predictive analytics in retailing. *Journal of Retailing*, *93*(1), 79–95. https://doi.org/10.1016/j.jretai.2016.12.004

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science*, *4*(3), 340–347. https://doi.org/10.1177/1948550612455931

Bryman, A. (2012). *Social research methods. Fourth edition. Oxford University Press, Oxford.* (Fourth). Oxford University Press.

Bughin, J., & Chui, M. (2010). The rise of the networked enterprise: Web 2.0 finds its payday. *McKinsey Quarterly*, *December*(22), 1–9.

Casas-Roma, J., Herrera-Joancomartí, J., & Torra, V. (2017). k-degree anonymity and edge selection: Improving data utility in large networks. *Knowledge and Information Systems*, *50*(2), 447–474. https://doi.org/10.1007/s10115-016-0947-7

Chen, D., Fraiberger, S. P., Moakler, R., & Provost, F. (2017). Enhancing transparency and control when drawing data-driven inferences about individuals. *Big Data*, *5*(3), 197–212. https://doi.org/10.1089/big.2017.0074

Cheng, X., Su, L., Luo, X. (Robert), Benitez, J., & Cai, S. (2021). The good, the bad, and the ugly: Impact of analytics and artificial intelligence-enabled personal information collection on privacy and participation in ridesharing. *European Journal of Information Systems*, *Latest Articles*(onlinefirst), 1–25. https://doi.org/10.1080/0960085X.2020.1869508

Child, J. T., Pearson, J. C., & 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), 2079–2094. https://doi.org/10.1002/asi.21122

Chin, W. W. (1998). Commentary: Issues and opinion on structural equation modeling. *MIS Quarterly*, *22*(1), vii–xvi. JSTOR.

Cichy, P., Torsten, O. S., & Kohli, R. (2014). Extending the privacy calculus: The role of psychological ownership. *Proceedings of the 35th International Conference on Information Systems*, *4*, 3010–3029.

Constant, D., Kiesler, S., & Sproull, L. (1994). What's mine is ours, or is it? A study of attitudes about information sharing. *Information Systems Research*, *5*(4), 400–421. Business Source Premier.

Corrigan, H. B., Craciun, G., & Powell, A. M. (2014). How does target know so much about its customers? Utilizing customer analytics to make marketing decisions. *Marketing Education Review*, *24*(2), 159–166. https://doi.org/10.2753/MER1052-8008240206

Davison, A. C., & Hinkley, D. V. (1997). *Bootstrap methods and their application*.

Dijkstra, T. K., & Henseler, J. (2015). Consistent partial least squares path modeling. *MIS Quarterly*, *39*(2), 297–316.

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, *22*(3), 295–316. https://doi.org/10.1057/ejis.2012.23

Dong, J. Q., & Yang, C.-H. (2020). Business value of big data analytics: A systems-theoretic approach and empirical test. *Information & Management*, *57*(1), 1–9. https://doi.org/10.1016/j.im.2018.11.001

Dong, W., Liao, S., & Zhang, Z. (2018). Leveraging financial social media data for corporate fraud detection. *Journal of Management Information Systems*, *35*(2), 461–487. https://doi.org/10.1080/07421222.2018.1451954

Duhigg, C. (2012, February 16). *How companies learn your secrets*. New York Times. https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html

Durcikova, A., Lee, A. S., & Brown, S. A. (2018). Making rigorous research relevant: Innovating statistical action research. *MIS Quarterly*, *42*(1), 241–263. https://doi.org/10.25300/MISQ/2018/14146

Dwork, C. (2011). A firm foundation for private data analysis. *Communications of the ACM*, *54*(1), 86–95. https://doi.org/10.1145/1866739.1866758

Dwork, C., & Roth, A. (2013). The algorithmic foundations of differential privacy. *Foundations and Trends in Theoretical Computer Science*, *9*(3–4), 211–407. https://doi.org/10.1561/0400000042

Efron, B., & Tibshirani, R. (1993). *An introduction to the bootstrap*. Chapman & Hall.

Ellemers, N., & Haslam, S. A. (2012). Social Identity Theory. In P. Van Lange, A. Kruglanski, & E. Higgins, *Handbook of theories of social psychology* (pp. 379–398). SAGE Publications Ltd. https://doi.org/10.4135/9781446249222.n45

Fan, W., & Gordon, M. D. (2014). The power of social media analytics. *Communications of the ACM*, *57*(6), 74–81. https://doi.org/10.1145/2602574

Faul, F., Erdfelder, E., Buchner, A., & Lang, A.-G. (2009). Statistical power analyses using G*Power 3.1: Tests for correlation and regression analyses. *Behavior Research Methods*, *41*(4), 1149–1160. https://doi.org/10.3758/BRM.41.4.1149

Fink, A. (2003). *The survey handbook*. SAGE Publications, Inc. https://doi.org/10.4135/9781412986328

Gabisch, A. J., & Milne, G. R. (2014). The impact of compensation on information ownership and privacy control. *Journal of Consumer Marketing*, *31*(1), 13–26. https://doi.org/10.1108/JCM-10-2013-0737

Giordano, A. P., Patient, D., Passos, A. M., & Sguera, F. (2020). Antecedents and consequences of collective psychological ownership: The validation of a conceptual model. *Journal of Organizational Behavior*, *41*(1), 32–49. https://doi.org/10.1002/job.2418

Gopal, R. D., Hidaji, H., Patterson, R. A., Rolland, E., & Zhdanov, D. (2018). How much to share with third parties? User privacy concerns and website dilemmas. *MIS Quarterly*, *42*(1), 143–164. https://doi.org/10.25300/MISQ/2018/13839

Graepel, T., Lauter, K., & Naehrig, M. (2013). ML Confidential: Machine Learning on Encrypted Data. In T. Kwon, M.-K. Lee, & D. Kwon (Eds.), *Information Security and Cryptology – ICISC 2012* (Vol. 7839, pp. 1–21). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-37682-5_1

Hair, J. F., Hult, G. T. M., Ringle, C., Sarstedt, M., Danks, N., & Soumya, R. (2022). *Partial least squares structural equation modeling (PLS-SEM) using R* (Third Edition). SAGE.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice*, *19*(2), 139–152. https://doi.org/10.2753/MTP1069-6679190202

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, *31*(1), 2–24. https://doi.org/10.1108/EBR-11-2018-0203

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of*

the Academy of Marketing Science, *43*(1), 115–135. https://doi.org/10.1007/s11747-014-0403-8

Hermes, S., Clemons, E. K., Wittenzellner, D., Hein, A., Böhm, M., & Krcmar, H. (2020). Consumer attitudes towards firms that monetize personal information: A cluster analysis and regulatory implications. *Proceedings of the 24th Pacific Asia Conference on Information Systems*, *1*, 1–14.

Hollenbaugh, E. E. (2019). Privacy management among social media natives: An exploratory study of Facebook and Snapchat. *Social Media + Society*, *5*(3), 1–13. https://doi.org/10.1177/2056305119855144

Holsapple, C. W., Hsiao, S.-H., & Pakath, R. (2018). Business social media analytics: Characterization and conceptual framework. *Decision Support Systems*, *110*, 32–45. https://doi.org/10.1016/j.dss.2018.03.004

Hong, W., & Thong, J. Y. L. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS Quarterly*, *37*(1), 275–298. JSTOR Journals.

Hu, Y., Xu, A., Hong, Y., Gal, D., Sinha, V., & Akkiraju, R. (2019). Generating business intelligence through social media analytics: Measuring brand personality with consumer-, employee-, and firm-generated content. *Journal of Management Information Systems*, *36*(3), 893–930. https://doi.org/10.1080/07421222.2019.1628908

Jarvenpaa, S. L., & Staples, D. S. (2001). Exploring perceptions of organizational ownership of information and expertise. *Journal of Management Information Systems*, *18*(1), 151–183. ProQuest One Academic.

Karahanna, E., Xin Xu, S., Xu, Y., & Zhang, N. (Andy). (2018). The needs–affordances–features perspective for the use of social media. *MIS Quarterly*, *42*(3), 737–756. https://doi.org/10.25300/MISQ/2018/11492

Kent, R. J., & Allen, C. T. (1994). Competitive interference effects in consumer memory for advertising: The role of brand familiarity. *Journal of Marketing*, *58*(3), 97. https://doi.org/10.2307/1252313

Kim, S. H., & Kwon, J. (2019). How do EHRs and a meaningful use initiative affect breaches of patient information? *Information Systems Research*, *30*(4), 1184–1202. https://doi.org/10.1287/isre.2019.0858

Kitchens, B., Dobolyi, D., Li, J., & Abbasi, A. (2018). Advanced customer analytics: Strategic value through integration of relationship-oriented big data. *Journal of Management Information Systems*, *35*(2), 540–574. https://doi.org/10.1080/07421222.2018.1451957

Koh, B., Raghunathan, S., & Nault, B. R. (2017). Is voluntary profiling welfare enhancing? *MIS Quarterly*, *41*(1), 23–41. https://doi.org/10.25300/MISQ/2017/41.1.02

Krasnova, H., & Veltri, N. F. (2010). Privacy calculus on social networking sites: Explorative evidence from Germany and USA. *Proceedings of the 43rd Hawaii International Conference on System Sciences*, *1*, 1–10. https://doi.org/10.1109/HICSS.2010.307

Kwon, S. (2020). Understanding user participation from the perspective of psychological ownership: The moderating role of social distance. *Computers in Human Behavior*, *105*, 106207. https://doi.org/10.1016/j.chb.2019.106207

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues*, *33*(3), 22–42. https://doi.org/10.1111/j.1540-4560.1977.tb01880.x

Li, T., Li, J., Liu, Z., Li, P., & Jia, C. (2018). Differentially private naive bayes learning over multiple data sources. *Information Sciences*, *444*, 89–104. https://doi.org/10.1016/j.ins.2018.02.056

Li, X.-B., & Qin, J. (2017). Anonymizing and sharing medical text records. *Information Systems Research*, *28*(2), 332–352. https://doi.org/10.1287/isre.2016.0676

Li, X.-B., & Raghunathan, S. (2014). Pricing and disseminating customer data with privacy awareness. *Decision Support Systems*, *59*, 63–73. https://doi.org/10.1016/j.dss.2013.10.006

Li, X.-B., & Sarkar, S. (2013). Class-restricted clustering and microperturbation for data privacy. *Management Science*, *59*(4), 796–812. https://doi.org/10.1287/mnsc.1120.1584

Li, X.-B., & Sarkar, S. (2014). Digression and value concatenation to enable privacy-preserving regression. *MIS Quarterly*, *38*(3), 679–698. https://doi.org/10.25300/MISQ/2014/38.3.03

Lowry, P. B., D'Arcy, J., Hammer, B., & Moody, G. D. (2016). "Cargo Cult" science in traditional organization and information systems survey research: A case for using nontraditional methods of data collection, including Mechanical Turk and online panels. *The Journal of Strategic Information Systems*, *25*(3), 232–240. https://doi.org/10.1016/j.jsis.2016.06.002

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336–355. https://doi.org/10.1287/isre.1040.0032

Martens, D., Provost, F., Clark, J., & Junqué de Fortuny, E. (2016). Mining massive fine-grained behavior data to improve predictive analytics. *MIS Quarterly*, *40*(4), 869–888. https://doi.org/10.25300/MISQ/2016/40.4.04

Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, *45*(2), 135–155. https://doi.org/10.1007/s11747-016-0495-4

Mason, W., & Suri, S. (2012). Conducting behavioral research on Amazon's Mechanical Turk. *Behavior Research Methods*, *44*(1), 1–23. https://doi.org/10.3758/s13428-011-0124-6

Montaquila, J. M., & Godwin, C. N. (2016). Personnel security and open source intelligence: Employing social media analytics in pre-employment screening and selection. *Journal of Information Privacy and Security*, *12*(3), 145–159. https://doi.org/10.1080/15536548.2016.1213997

Narayanan, A., & Shmatikov, V. (2006). How to break anonymity of the Netflix prize dataset. *Computing Research Repository*. http://arxiv.org/abs/cs/0610105

Nunally, J. C. (1978). *Psychometric theory*. McGraw-Hill.

Pavlou. (2011). State of the information privacy literature: Where are we now and where should we go? *MIS Quarterly*, *35*(4), 977. https://doi.org/10.2307/41409969

Pavlou, Liang, & Xue. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS Quarterly*, *31*(1), 105. https://doi.org/10.2307/25148783

Petronio, S. S. (2002). *Boundaries of privacy dialectics of disclosure*. State University of New York Press. http://site.ebrary.com/id/10587254

Pierce, J. L., Kostova, T., & Dirks, K. T. (2001). Toward a theory of psychological ownership in organizations. *The Academy of Management Review*, *26*(2), 298. https://doi.org/10.2307/259124

Pole, A. (2010, October 19). *How Target gets the most out of its guest data*. Predictive Analytics World. https://www.predictiveanalyticsworld.com/machinelearningtimes/how-target-gets-the-most-out-of-its-guest-data-to-improve-marketing-roi/6815/

Poom, A., Järv, O., Zook, M., & Toivonen, T. (2020). COVID-19 is spatial: Ensuring that mobile big data is used for social good. *Big Data & Society*, *7*(2), 1–7. https://doi.org/10.1177/2053951720952088

Reynolds, K. J. (2017). Self-categorization theory. In B. S. Turner (Ed.), *The Wiley-Blackwell Encyclopedia of Social Theory* (pp. 1–4). John Wiley & Sons, Ltd. https://doi.org/10.1002/9781118430873.est0327

Ringle, C. M., Wende, S., & Becker, J.-M. (2015). *SmartPLS*. https://www.smartpls.com/documentation/algorithms-and-techniques/bootstrapping/

Ringle, Sarstedt, & Straub. (2012). Editor's comments: A critical look at the use of PLS-SEM in "MIS Quarterly." *MIS Quarterly*, *36*(1), iii. https://doi.org/10.2307/41410402

Sarstedt, M., & Cheah, J.-H. (2019). Partial least squares structural equation modeling using SmartPLS: A software review. *Journal of Marketing Analytics*, *7*(3), 196–202. https://doi.org/10.1057/s41270-019-00058-3

Sarstedt, M., Hair, J. F., Nitzl, C., Ringle, C. M., & Howard, M. C. (2020). Beyond a tandem analysis of SEM and PROCESS: Use of PLS-SEM for mediation analyses! *International Journal of Market Research*, *62*(3), 288–299. https://doi.org/10.1177/1470785320915686

Sekaran, U., & Bougie, R. (2019). *Research methods for business: A skill-building approach*. John Wiley & Sons, Incorporated. https://books.google.com/books?id=nkv1xwEACAAJ

Sharma, S., & Crossler, R. E. (2014). Intention to engage in social commerce: Uses and gratifications approach. *Proceedings of the 20th Americas Conference on Information Systems*, *5*, 3756–3767.

Shmueli, G., Ray, S., Velasquez Estrada, J. M., & Chatla, S. B. (2016). The elephant in the room: Predictive performance of PLS models. *Journal of Business Research*, *69*(10), 4552–4564. https://doi.org/10.1016/j.jbusres.2016.03.049

Shokri, R., & Shmatikov, V. (2015). Privacy-preserving deep learning. *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 1310–1321. https://doi.org/10.1145/2810103.2813687

Singel, R. (2009, December 17). *Netflix spilled your brokeback mountain secret, lawsuit claims*.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, *35*(4), 989–1015. https://doi.org/10.2307/41409970

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, *20*(2), 167. https://doi.org/10.2307/249477

Social connectedness Index – Facebook data for good. (2021, July 18). Facebook Data for Good. https://dataforgood.fb.com/tools/social-connectedness-index/

Suseno, Y., Laurell, C., & Sick, N. (2018). Assessing value creation in digital innovation ecosystems: A social media analytics approach. *The Journal of Strategic Information Systems*, *27*(4), 335–349. https://doi.org/10.1016/j.jsis.2018.09.004

Sweeney, L. (2002). Achieving k-anonymity privacy protection using generalization and suppression. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, *10*(05), 571–588. https://doi.org/10.1142/S021848850200165X

Tajfel, H. (1974). Social identity and intergroup behavior. *Social Science Information*, *13*(2), 65–93.

Tanner, A. (2016, January 19). *How data brokers make money off your medical records*. Scientific American. https://doi.org/10.1038/scientificamerican0216-26

Terrell, S. R. (2015). *Writing a proposal for your dissertation: Guidelines and examples*. Guilford Publications. https://books.google.com/books?id=blauCgAAQBAJ

Tran, H.-Y., & Hu, J. (2019). Privacy-preserving big data analytics a comprehensive survey. *Journal of Parallel and Distributed Computing*, *134*, 207–218. https://doi.org/10.1016/j.jpdc.2019.08.007

Tsai, H.-T., & Bagozzi, R. P. (2014). Contribution behavior in virtual communities: Cognitive, emotional, and social influences. *MIS Quarterly*, *38*(1), 143–164.

Turner, J. C., & Reynolds, K. J. (2012). Self-categorization theory. In P. A. M. Van Lange, A. W. Kruglanksi, & E. T. Higgins (Eds.), *Handbook of Theories of Social Psychology* (Vol. 2, pp. 399–417). Sage Publications.

Vannucci, V., & Pantano, E. (2020). Do I lose my privacy for a better service? Investigating the interplay between big data analytics and privacy loss from young consumers' perspective. In E. Pantano (Ed.), *Retail Futures* (pp. 193–205). Emerald Publishing Limited. https://doi.org/10.1108/978-1-83867-663-620201021

Wang, Q., He, M., Du, M., Chow, S. S. M., Lai, R. W. F., & Zou, Q. (2018). Searchable encryption over feature-rich data. *IEEE Transactions on Dependable and Secure Computing*, *15*(3), 496–510. https://doi.org/10.1109/TDSC.2016.2593444

Wang, X., Mu, Y., & Chen, R. (2017). Privacy-preserving data search and sharing protocol for social networks through wireless applications. *Concurrency and Computation: Practice and Experience*, *29*(7), 1–24. https://doi.org/10.1002/cpe.3870

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, *4*(5), 193. https://doi.org/10.2307/1321160

Watson, R. T., & Webster, J. (2020). Analysing the past to prepare for the future: Writing a literature review a roadmap for release 2.0. *Journal of Decision Systems*, *29*(3), 129–147. https://doi.org/10.1080/12460125.2020.1798591

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, *26*(2), xiii–xxiii. JSTOR.

Wedel, M., & Kannan, P. K. (2016). Marketing analytics for data-rich environments. *Journal of Marketing*, *80*(6), 97–121. https://doi.org/10.1509/jm.15.0413

Westin, A. F. (1967). *Privacy and freedom*. Atheneum, New York.

White, T. B., Zahay, D. L., Thorbjørnsen, H., & Shavitt, S. (2008). Getting too personal: Reactance to highly personalized email solicitations. *Marketing Letters*, *19*(1), 39–50. https://doi.org/10.1007/s11002-007-9027-9

Wieringa, J., Kannan, P. K., Ma, X., Reutterer, T., Risselada, H., & Skiera, B. (2021). Data analytics in a privacy-concerned world. *Journal of Business Research*, *122*, 915–925. https://doi.org/10.1016/j.jbusres.2019.05.005

Wong, K. K.-K. (2019). *Mastering partial least squares structural equation modeling (PLS-SEM) with SmartPLS in 38 hours*. IUniverse.

Yang, J., Wang, B., Yang, X., Zhang, H., & Xiang, G. (2014). A secure k-automorphism privacy preserving approach with high data utility in social networks: A secure k-automorphism privacy preserving approach. *Security and Communication Networks*, *7*(9), 1399–1411. https://doi.org/10.1002/sec.840

Ying, X., & Wu, X. (2011). On link privacy in randomizing social networks. *Knowledge and Information Systems*, *28*(3), 645–663. https://doi.org/10.1007/s10115-010-0353-5

Yun, H., Lee, G., & Kim, D. J. (2019). A chronological review of empirical research on personal information privacy concerns: An analysis of contexts and research constructs. *Information & Management*, *56*(4), 570–601. https://doi.org/10.1016/j.im.2018.10.001

Zetter, K. (2009, June). *Lawsuit accuses Facebook of conspiring to break video-privacy law*. https://www.wired.com/2009/11/beacon/

Zhang, J., Sun, J., Zhang, R., Zhang, Y., & Hu, X. (2018). Privacy-preserving social media data outsourcing. *Proceedings of the IEEE Conference on Computer Communications*, 1106–1114. https://doi.org/10.1109/INFOCOM.2018.8486242

Zhao, C., Zhao, S., Zhao, M., Chen, Z., Gao, C.-Z., Li, H., & Tan, Y. (2019). Secure multi-party computation: Theory, practice and applications. *Information Sciences*, *476*, 357–372. https://doi.org/10.1016/j.ins.2018.10.024

Zhu, Y.-Q., & Kanjanamekanant, K. (2020). No trespassing: Exploring privacy boundaries in personalized advertisement and its effects on ad attitude and purchase intentions on social media. *Information & Management*, *58*(2), 1–10. https://doi.org/10.1016/j.im.2020.103314