

2022

Factors Affecting Customers' Decision to Share Personal Data with Mobile Operators

Ammar Ali Qaffaf

Follow this and additional works at: https://nsuworks.nova.edu/gscis_etd



Part of the [Community-Based Research Commons](#), [Computer Sciences Commons](#), and the [Library and Information Science Commons](#)

Share Feedback About This Item

This Dissertation is brought to you by the College of Computing and Engineering at NSUWorks. It has been accepted for inclusion in CCE Theses and Dissertations by an authorized administrator of NSUWorks. For more information, please contact nsuworks@nova.edu.

Factors Affecting Customers' Decision to Share Personal Data with
Mobile Operators

by

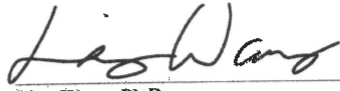
Ammar Qaffaf

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in
Information Systems

College of Computing and Engineering
Nova Southeastern University

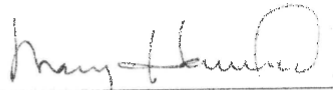
2022

We hereby certify that this dissertation, submitted by Ammar Qaffaf 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

1/31/22
Date



Mary Harward, Ph.D.
Dissertation Committee Member

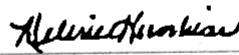
1/31/22
Date



Junping Sun, Ph.D.
Dissertation Committee Member

1/31/22
Date

Approved:



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

1/31/22
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

Factors Affecting Customers' Decision to Share Personal Data with Cellular Service Providers

by
Ammar Qaffaf
January 2022

Companies that personalize their services based on users' specific needs have increased sales and customer satisfaction. Personalization requires analyzing the user's behavior and correlating the action with other pieces of information. The information available for cellular service providers has grown substantially as connectivity becomes ubiquitous. Customers are unknowingly sharing their locations, habits, activities, and preferences in real-time with their service providers. Although cellular service providers state that they share personal data with external entities in their publicly available privacy policies, users have limited control over who can access their personal information. Users have no, or suboptimal, control to manage their information sharing. The limitation of this control includes a lack of flexibility to exclude specific times, events, or third-party entities that ends up receiving their data. Customers' willingness to share their information with cellular service providers has not been examined to date. Therefore, this study used a custom mobile application to address the lack of control in sharing information with cellular service providers. The application generated nudges to allow for more informed privacy decisions by (a) increasing users' awareness of the data shared with their cellular service providers and (b) providing users the option not to share their personal information if desired. The elaboration likelihood model (ELM), a dual-route, multi-process decision-making model, was utilized to develop a theoretical model to investigate the willingness to share personal data with cellular service providers. The factors that influence users' attitudes and behaviors toward information sharing were explored. The study findings suggest a negative influence of the awareness of the privacy practices taken by the cellular service providers on the intention to share personal information, proving that those who know how their data is collected and used are less inclined to share. The study results revealed that the intention to share personal information positively influences the actual information sharing based on the responses to the privacy nudges, unlike the common belief that people only talk about the need to protect their data but eventually give it away when asked. This study suggests otherwise; those who want to protect their data will protect them if they were given a choice. This study concluded that using a mobile application that nudges users to accept or reject information sharing would reduce information sharing by 42%. A higher awareness of service providers' privacy practices resulted in decreased sharing of personal information. This study highlighted the trade-off between information sharing and the benefits of personalization. Practical guidance on enhancing user privacy attitudes regarding sharing personal data with cellular service providers was discussed.

Acknowledgments

I want to express my deepest gratitude to my mentor, advisor, and committee chair, Dr. Ling Wang, for her excellent guidance, dedication, unconditional support, and genuine passion for the best research outcome. I would also like to thank my dissertation committee members, Dr. Mary Harward and Dr. Junping Sun, who continuously provided detailed feedback and overwhelmed me with their support over the past few years.

I am forever grateful to my wife, Carmel, who has always stood by me and cheered me up through the many difficulties we faced together, and to my kids (Ali and Remi) who have been the light at the end of the tunnel when it seemed impossible to move forward.

I would have never been able to complete this work without the unlimited support and encouragement from my parents (Ali and Amal), sisters (Esraa, Bayan, Heba, and Haneen), and my brothers (Mohammad and Asem).

Finally, praise be to God for giving me the ability and power to complete this degree.

Table of Contents

Abstract iii

List of Tables vii

List of Figures viii

Chapters

Chapter 1 Introduction 1

Background 1

Problem Statement 2

Dissertation Goal 5

Study Framework 7

Research Question 9

Hypotheses 9

Relevance and Significance 12

Barriers and Issues 14

Assumptions, Limitations, and Delimitations 15

Definitions of Terms 15

Chapter 2 Review of the Literature 17

Introduction 17

Personally Identifiable Information 17

Privacy and Personalization 18

The Economics of Privacy 19

Cellular Service Providers 20

Privacy and Legal 22

Privacy Enhancing Technologies (PETs) 26

Relevant Research 27

Theoretical Foundation 33

Chapter 3 Research Methodology 37

Overview 37

Research Design 37

Mobile Application 40

Sampling Methods 42

Instrument Development and Validation 42

Recruitment 47

Data Collection Procedures 48

Data Analysis Strategies 48

Summary 49

Chapter 4 Results 50

Overview 50

Data Collection 50

Data Screening 52

Demographic Analysis 53

Survey 58
Findings 61
Summary 70

Chapter 5 Conclusions, Implications, Recommendations, and Summary 72

Conclusions 72
Implications 75
Limitations 76
Recommendations 77
Summary 78

Appendix A Questionnaire 79

Appendix B Institutional Review Board 96

References 98

List of Tables

Tables

1. Relevant Literature Review Summary 28
2. Sociodemographic Characteristics of Survey Participants 54
3. Cellular Phone Service Characteristics 57
4. Construct Reliability: First Approach (n = 791) 58
5. Construct Reliability and Validity: Second Approach (n = 118) 59
6. Heterotrait-Monotrait (HTMT) Ratio of Correlations 60
7. One-Sample Proportions Confidence Intervals 61
8. Hypothesis Test Using One-Sample Binomial Test 63
9. Decline and Approval Percentage of Privacy Nudges 65
10. Mann-Whitney Ranks for the Age Groups and Nudges 66
11. Mann-Whitney U Test of the Moderating Role of Age: Fourth Hypothesis 67
12. Path Coefficients: Second Approach (n = 118) 68

List of Figures

Figures

1. Conceptual Research Model 8
2. Samples of the Nudges 41
3. Android Mobile Application Home Page (First and Second Approaches) 52
4. One-Sample Binomial Test for the nudges and the hypothesized percentages 62
5. Path Coefficients (n=118) 69
6. PLS Analysis Showing Path Coefficients and Cronbach's Alpha for the
Constructs 70

Chapter 1

Introduction

Background

The United States is the third-largest country in terms of cellular users, with a total subscribership of 345,225,000 at the end of 2018 (Snyman, 2021). Cellular service providers access personal information to serve customers. AT&T and Verizon's privacy policies show both companies collect and process personal data without user consent (Cranor et al., 2018). Cellular service providers may use personal information for purposes that users may not desire, such as personalization and advertising (Ohm, 2010; The Radicati Group Inc., 2019).

Cellular phone users have limited control over service providers' access to their personal information (Tene & Polonetsky, 2013). Data privacy laws require that users provide explicit consent before service providers can collect, process, or sell user data. Telecommunication companies have used deidentification for analytics while preserving individuals' privacy. Lawmakers have accepted this practice over the past 40 years. However, with the recent advancements in computing power, companies can reidentify anonymized data and associate them with specific individuals (Choi et al., 2019; U.S. Senate Committee on Commerce, Science, and Transportation, 2019).

Anonymization is a process in which personally identifying information, such as names and social security numbers, is deleted to protect individuals' privacy in large databases. Ohm (2010) demonstrated that it is possible to reidentify individuals hidden in anonymized data with astonishing ease. Therefore, companies should not overlook

the importance of user consent before collecting personal information, even if anonymized. Nudges were proposed as a soft-paternalistic behavioral intervention method to direct the user toward a better privacy attitude. However, nudges rely on the heuristic cognitive processes that the brain uses when a quick decision is required or when an incomplete set of information is available. This study analyzed the amount and type of requested personal information, the trust level with the service provider, and the heuristic nudges that stimulate rational decision-making processes (Acquisti, 2009; Acquisti et al., 2013; Acquisti & Grossklags, 2012; Choi et al., 2019; Golle, 2006; Larose & Rifon, 2006; Mohr et al., 2019; Mraznica, 2017).

Problem Statement

Most studies on personal data sharing assume that users' decisions are driven by either an influential belief that is created through deliberative cognitive processes (Awad & Krishnan, 2006; Chellappa, 2002; Kobsa et al., 2016; Li & Unger, 2012) or by an emotional shortcut that focuses on the attributes of the request (Acquisti, 2009; Acquisti et al., 2013; Acquisti & Grossklags, 2012; Larose & Rifon, 2006). Few studies have considered integrating both assumptions (Ho & Bodoff, 2014; Kobsa et al., 2016). Furthermore, many privacy studies have investigated personal data sharing among smartphone application developers (Gu et al., 2017; Palmerino, 2018; Peruma et al., 2018; Saborido et al., 2017) and social media companies (Garg et al., 2014; Hsu & Wu, 2012; Pitkänen & Tuunainen, 2012; Waldman, 2016), while the personalization versus privacy paradox in services provided by telecommunication companies has not been examined to date. This study aimed to reconcile rational privacy calculus and heuristic decisional shortcuts when sharing personal information with cellular service providers.

Privacy literature contains broadly contradictory recommendations for enhancing privacy-related behaviors and attitudes. Li and Unger (2012) argued that companies should be more transparent when requesting personal data by detailing information requests and information sharing benefits. On the other hand, Acquisti (2013) and Bal et al. (2011) suggested that companies should reduce their transparency and user control. Acquisti et al. (2013) found that presenting the user with a privacy notice has only a positive effect for only 15 seconds. They argued that the 15-second delay is much shorter than the delay between users reading the privacy policy, if they do, and the interaction with the provider services. Similarly, Bashir et al. (2014) and Acquisti et al. (2016) found that transparency and control could produce negative results and lead to riskier disclosures. They found that providing users with more information on why they should not share information actually leads to people oversharing their personal information.

Lowry et al. (2012) and Bal et al. (2011) provided a theoretical discussion of the privacy literature's apparent contradictory recommendations. Lowry et al. (2012) examined the persuasiveness of website privacy assurance cues for consumers and demonstrated that prior findings were not necessarily contradictory when considered using the elaboration likelihood model (ELM). The ELM suggests that the decision-making process involves both central and peripheral routes. In the central route, the user logically processes the presented arguments to make a decision, which justifies the need for more details. In the peripheral route, the user makes their decision based on the presented message at the time and predetermined rules without considering their

surroundings, meaning that more details could produce a negative result (Ho & Bodoff, 2014).

Individual perceptions and emotional reactions play a prominent role in influencing attitudes and behaviors (Pentina et al., 2016). Users find it difficult to make systematic cost-benefit evaluations before making spontaneous decisions to protect their privacy. Therefore, users require an external support system to make quick decisions regarding information disclosure. Studies on privacy-enhancing technologies have proposed soft paternalism strategies to nudge users toward sharing less personal information with minimal cognitive effort and biases (Zhang & Xu, 2016). However, Sætra (2019) found that using advancements in big data, privacy nudges can be both manipulative and coercive, which can severely impact people's liberty by manipulating users' behavior to follow the best interest of the companies rather than the users.

Privacy nudges by companies requesting information particularize the personal information request. The transparency offered by the nudges allows users to understand the amount and type of personal data being accessed. The amount and type of data requested by the service provider may affect a person's decision to share their data. Tene and Polonetsky (2013) found that companies that request more data can incite suspicion and affect user decisions to share data. This construct affects the type of information that can be deduced later from the consumer and the extent to which this information can expose the user to the public oversight (Pitkänen & Tuunainen, 2012).

Trust is defined as the level at which people believe a firm is able to protect their information. Cellular service providers are known for their brands and big advertising budgets; therefore, trust is a critical element when users evaluate the exchange of their

data for potential benefits (Dogruel et al., 2017). Users' trust level toward the company is essential, and their prior experiences with the company's data requests are crucial to their willingness to provide personal information. Companies can rely on existing relationships with users to ensure that their data collection requests are not considered suspicious. The entity receiving the data and the nature of the user-entity relationship affect users' perceptions of potential privacy violations (Miltgen, 2009).

Prior research examined the myriad factors that influence users' desire to share personal data. Milberg et al. (1995) found that the level of personal information privacy concerns varies based on nationality and cultural values. Chakraborty and Tripp (2016) focused on eavesdropping from mobile applications that collect and share personal data with untrustworthy third parties as an information privacy concern and proposed a framework to provide users with better control over their personal information. Miaoui et al. (2015) examined the effect of weak security systems on data privacy economics. Robinson (2018) investigated the direct influence of anxiety, personality, and perceived benefits on attitudes toward self-detection. Pu and Grossklags (2019) analyzed the impact of anonymity on privacy decision-making. To the best of the researcher's knowledge, the present study is the first to bridge the scientific gap in the privacy field by addressing the influencing variables, amount and type of requested information, company trust level, and privacy nudges in a context related to cellular service providers.

Dissertation Goal

One puzzling question in the privacy literature is why people disregard privacy concerns and willingly share data with external entities despite publicly stated

opposition and concerns about privacy loss. This study aimed to use firsthand data to analyze customers' decisions to share personal data with cellular service providers and the factors that influence that decision. A conceptual model was created, and hypotheses were designed to measure the relative impact of the proposed constructs on consumers' willingness to share data with cellular service providers. More broadly, the study sought to offer recommendations to help consumers achieve a balance in information sharing by receiving the benefits of personalized services from cellular service providers.

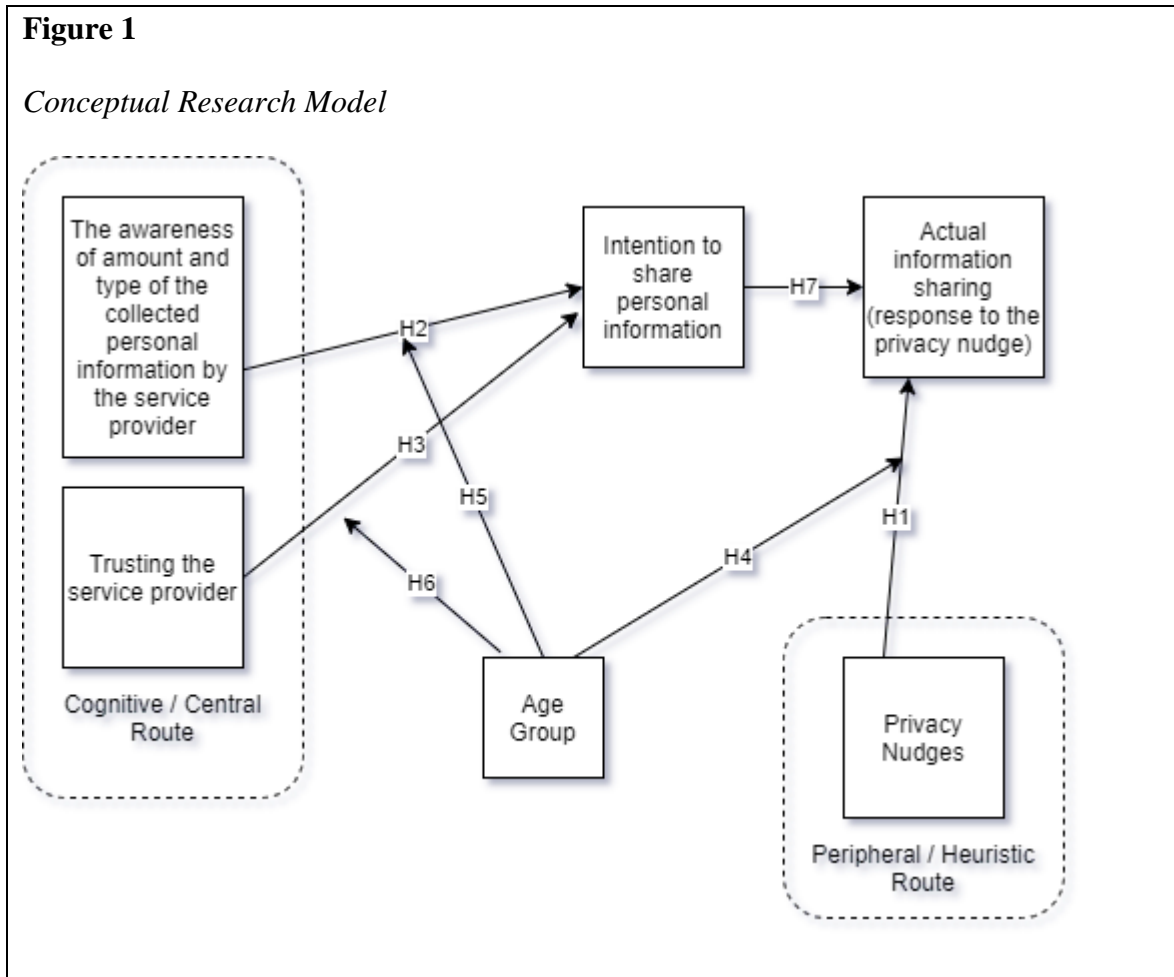
While nudges are becoming increasingly popular privacy tools for decision-making (Milberg et al., 1995; Thunström et al., 2018), they influence only individuals' mental shortcut decision-making processes (Wang et al., 2014). This study employed ELM as the theoretical foundation to overcome the limitations of nudges. The ELM postulates that information processing occurs through central and peripheral routes, which differ in the amount of cognitive elaboration. Drawing on the ELM, this study conceptualized the amount and type of requested data and the company trust level as the two central cues. The presence and quality of privacy nudge subtly influence users' decisions.

It was predicted that age groups would play a moderating role in both the central and peripheral routes. Users who perceive the information as relevant to their age group may be influenced through the cognitive route. Otherwise, users may make decisions through the peripheral path. Older users may form privacy decisions based on prior experiences or historical events related to the company (Bal et al., 2011). Rodríguez-Priego et al. (2016) concluded that younger participants were more likely to disclose personal information than older participants. However, the influence of age on the

effectiveness of the privacy nudges, the amount and type of requested personal information, and the trust level towards the service provider in this study is unclear.

Study Framework

The dual-route ELM was applied to examine personalization versus privacy behavior by integrating the rational privacy-calculus route. Once the nudge is presented, the participant has to decide whether to accept sharing their personal data. The *rational* decision-making process requires the user to process the amount and type of personal information requested and their trust in the company. Some nudges were presented when the cellular service provider accessed customer data represented the decisional-shortcut route and lacked informational messages about the requested data. Participant demographics, namely age, served as a moderating variable. This study was one of few studies to observe actual data-sharing behavior in an interactive environment that simulated reality. Most of the prior literature detailed data-sharing attitudes in hypothetical situations and used generic surveys focusing on behavioral intention rather than actual behavior (Kobsa et al., 2016).



The study framework summarized the literature review and created the tools required to test the hypotheses. The research model was based on the ELM, which states that people's motivation and ability influence their processing depth. The ELM is a dual process of attitude formation and decision-making that integrates decision-making processes with different degrees of elaboration. Therefore, it can be assumed that a person's decision to share personal information with a cellular service provider is influenced by instrumental beliefs constructed through deliberative cognitive processes. The central route was represented by the amount and type of personal data and the user's trust toward the company requesting information. The peripheral path was

characterized by the presence and quality of privacy nudges that formed a heuristic shortcut.

Research Question

RQ1: What factors influence users' decisions to share personal information with cellular service providers?

Hypotheses

Bashir et al. (2014) highlighted the importance of privacy nudges in shaping users' decisions to share their private data based on pre-existing knowledge levels. They demonstrated that privacy notices affected user behavior and suggested strengthening the significance of privacy nudges by altering the presentation, structure, frequency, and language to help consumers benefit from privacy notifications. Ambiguous nudges have adverse effects (Thunström et al., 2018). Milne and Culnan (2004) found that the control of personal information sharing was the main reason users read notices, particularly when asked to disclose sensitive information. Similarly, Tanaiutchawoot et al. (2019) revealed that nudges had a high potential to alter human decision-making behavior. Thus, the following hypothesis was formulated:

H1: More informed privacy nudges negatively influence customer choices to share personal information with the cellular service provider.

The amount and type of requested data may affect a person's decision to share information with companies. Users become suspicious when companies ask for a sizable amount of personal information, and companies that demand a large amount of data affect the perceived sensitivity of personal data. Consumers worry about the type of information that can be inferred from personal data, the extent to which the disclosure of

this information can expose them to public oversight, and the actions that can then be taken against them (Pitkänen & Tuunainen, 2012). Thus, the second hypothesis was:

H2: Customers are more likely to reject sharing data with companies that request larger amounts and more sensitive personal data.

Users' experience with the company requesting data is a critical factor in their willingness to share it. Companies rely on existing relationships to ensure that data collection requests are not considered questionable. The nature of the relationship between the company and the customer influences users' perceptions of potential privacy violations. Consumers' experiences with the company constitute their assessment of the risks posed by data disclosure, particularly concerning confidentiality. Consumers' previous experiences with the company influence their ability to trust the company to use the disclosed data appropriately (Miltgen, 2009; Waldman, 2016).

Therefore, the third hypothesis was as follows:

H3: Trust toward the cellular service provider is positively associated with the propensity to share personal information.

People from different age groups tend to exhibit varied behaviors toward external influences. Older individuals could have predetermined mental privacy shortcuts based on prior experiences, whereas younger people might be more receptive to external catalysts, such as privacy nudges. Therefore, the fourth hypothesis was:

H4: Age moderates the effect of privacy nudges on information sharing.

Older people might attribute less value to personalization than younger people, particularly when a large amount of personal data is required. Rodríguez-Priego et al. (2016) and Pu and Grossklags (2019) concluded that younger participants were more

likely to disclose and share sensitive information than older participants. Thus, the fifth hypothesis was:

H5: Age moderates the effect of the amount and type of requested data on information sharing.

People develop fewer social contacts later in adulthood (Zulas et al., 2014). Older people tend to be satisfied with their existing relationships. Emotional goals become more critical in middle adulthood, and the ability to create new relationships decreases. Consequently, relationships with external entities become more critical among older people. Trust could become more salient for older people, who could quickly lose trust when dealing with adverse events related to a particular company. This contradicts the general concept of lifespan psychology, which states that older people are better at regulating their emotions (Bal et al., 2011; Räsänen & Koiranen, 2016; Rasi & Kilpeläinen, 2016). Thus, the sixth hypothesis was:

H6: Age moderates an individual's trust level toward the company regarding information sharing.

Personal information sharing was measured by both the intention to share, following an adaption of the Internet Users' Information Privacy Concerns (IUIPC) scale developed by Malhotra et al. (2004), and the actual information sharing represented by the actual response to the privacy nudge. It is hypothesized that the intention and the actual information sharing are positively related; thus, the seventh hypothesis was:

H7: The intention to share personal information is positively associated with the actual information sharing.

Relevance and Significance

In the digital communication era, the relationship between businesses, consumers, and governments has become one of the most controversial privacy literature issues. Companies view consumers' privacy as a commodity, consumers perceive privacy as a right, and governments are in limbo between self-regulation effectiveness and enforcing legislation to protect citizens' privacy (Milberg et al., 1995; Slot, 2017).

Customers want the ability to decline sharing data that could reveal private life details, including their social circle, movements, socioeconomic class, and habits. If sensitive data are exposed, the fear of psychological impact promotes caution in sharing information. Customers become concerned if sensitive information is disclosed publicly (Leon et al., 2013; Martin et al., 2017; Waldman, 2016); however, most users opt to share sensitive data. Zhang and Xu (2016) found that 91% of mobile application users agreed to share their location information with application developers without clearly understanding how their data were being used. Consumers are keen to exercise control of their data, particularly when sensitive information is involved (Milne & Culnan, 2004); however, not all users read the policies to understand how their data will be used (Acquisti, 2009). Shih et al. (2015) found that users were more likely to share personal information when presented with a notification that explained the details and reason for the request.

Mousavi et al. (2020) explained oversharing behavior through the privacy calculus paradox. People are willing to trade off the potential privacy loss with the personalization benefit they expect to receive (Pentina et al., 2016). Similarly, Pu and

Grossklags (2019), Brandtzaeg et al. (2019), and Acquisti and Grossklags (2012) found that consumers' decisions may be influenced by the perceived benefits they expect, which form an essential factor in the privacy decision-making process. Slot (2017) demonstrated that over 90% of consumers share personal data with advertisers in exchange for highly personalized advertisements, while 50% of participants had a positive reaction when presented with personalized ads, indicating that most people are willing to put aside their privacy concerns and share more data for a better online experience.

The privacy calculus paradox has been tested on social networking sites (Krasnova & Veltri, 2010), mobile applications across the United States and China (Pentina et al., 2016), and e-commerce sites (Dinev & Hart, 2006). However, the privacy calculus has not yet been tested for cellular service providers. Rao et al. (2016) demonstrated that customers could not abstain from sharing their physical location or personally identifying information with cellular service providers, partially due to deficiencies in the design and structure of wireless networks, which did not prioritize privacy. Rao et al. (2016) proposed a potential countermeasure to defend users' privacy by introducing additional expensive modules to wireless networks.

However, wireless service providers have not implemented any privacy-enhancing measures (Huang & Bashir, 2016; P. Zhao et al., 2018). Wagner and Eckhoff (2018) found that cellular companies regularly access non-public user information, regardless of user preference or consent. Moreover, wireless networks are subject to multiple design flaws, leading to security issues that affect user privacy (Abdelrazek &

Azer, 2019). Even the latest fifth-generation cellular services offer limited privacy protection regarding location, identity, and data privacy (Liyanage et al., 2018).

Regulations have historically forced telecommunication companies to store all user data, as law enforcement agencies could use call records and customers' historic locations to investigate crimes or as evidence in court proceedings. However, the same data, stored for a longer time, can reveal intimate life details of individuals, including their habits, social circle, socioeconomic class, and transportation choices (Agarwal et al., 2012; Hermet & Combet, 2011; Sujata et al., 2015).

Cellular service providers are highly trusted (Bodi et al., 2010); therefore, customers are willing to share more data with them than with other companies. This trust has given cellular service providers access to data unavailable elsewhere, which could be used to generate profits. Cellular service providers sell these data to advertisers who are willing to pay a premium to increase the effectiveness of their marketing campaigns (Agarwal et al., 2012; Hong & Dietze, 2019; Minonne et al., 2018; Sujata et al., 2015).

This study was critical, as it highlighted a crucial topic and identified the elements that influence individual decisions to share data with cellular service providers. A literature review on this topic revealed that no prior studies had examined the impact of these building blocks on cellular service providers in particular. Thus, this study fills this gap in the literature.

Barriers and Issues

A pilot test to examine the mobile application and survey was conducted with a small sample of four participants selected through convenience sampling. Due to the

influence of the COVID-19 pandemic, the study was conducted remotely through teleconferences and mobile phone screen sharing.

Requesting users to complete a survey and then download and install a new mobile application on their smartphones was challenging. Some crowdsourced participants may complete the study using random data. This potential issue required quality control on the survey tool, including setting a time before any question can be answered to encourage consideration before answering.

Assumptions, Limitations, and Delimitations

Although the mobile application did not share any personal information with the researchers, people may be anxious about installing a new application on their phones. Quay-de la Vallee et al. (2016) used Amazon's Mechanical Turk (MTurk) to recruit participants who used and rated a mobile application and checked available human intelligence tasks (HITs). They found that few tasks involved installing mobile applications, including the Coultedd, which asks participants to install a private Android browser and provide feedback. Quay-de la Vallee et al. (2016) allocated 240 minutes to the task, which aligned with the timing in the present study.

Definitions of Terms

The below list of terms represents the main concepts in this research.

Privacy nudges are methods that drive an individual choice in a particular direction without eliminating the user's freedom of choice (Creswell, 2014). Privacy nudges are a method of predictably influencing personal choices toward making better privacy decisions and avoiding potential threats.

Personalization is the ability to tailor the product or purchase experience based on the individual consumer's taste, which cannot be done without specific information about the individuals (Chellappa & Sin, 2005).

Personally identifiable information (PII) is the information that can be used to identify or trace a distinct individual either alone or in combination with other publicly available information that can be linked to a specific individual (Vishwamitra et al., 2017).

Deep packet inspection (DPI) is a network device that provides access to the detailed content of the internet user traffic, including visited pages and applications.

Chapter 2

Review of the Literature

Introduction

This chapter summarizes existing research on privacy protection in interacting with businesses. First, privacy research drivers and the importance of privacy research are overviewed. Next, the measures taken by companies and governments to protect consumer privacy are reviewed. Finally, relevant studies are summarized, past information systems are detailed, and potential future information systems that could be used to create a more privacy-aware environment are discussed.

Personally Identifiable Information

People typically associate PII with personal details, such as Social Security Numbers (SSN), full name, health records, and other similar information. People often do not realize that companies use technology to pinpoint individuals by linking multiple nonpersonal details. Ohm (2010) demonstrated how companies that use deidentifying techniques could use zip code, birth date, and gender to uniquely identify any individual in the United States. Similarly, group photos on social media sites can be converted into PII and linked to an individual's identity (Vishwamitra et al., 2017).

Data directly collected by companies based on customer interactions are called first-party data. Many companies do not have sufficient first-party data on new customers or potential customers; therefore, they seek to supplement and enhance the value of their customer-level data by acquiring data from other companies. Some companies sell first-party data directly to other companies, referred to as second-party

data by the receiving company. Other companies collect data from various sources, including first-party data from other firms, aggregate the data by linking an individual's information from multiple sources into a single unit, and market these enriched user information units to other firms. The data that is sold by data aggregators are referred to as third-party data. The increasing demand for personalization has increased customer data value, contributing to the growth and success of companies that collect and market personal information (Schneider et al., 2017).

Privacy and Personalization

Privacy is a right granted by law. Privacy appears simple in everyday interactions; however, it is challenging to define privacy, as it represents different things to different people. Acquisti et al. (2016) described privacy as protecting someone's personal space, their right to be left alone, and control over the safeguarding of one's personal information. One expects their business and financial dealings with banks and other companies to remain private, as the exchange of personal details formulates a trust contract between the two parties. This trust contract is based on the condition that the second party will only use personal data for tasks that the first party receives consent for (Cadzow, 2012).

Personalization is the ability to proactively tailor products and purchasing experience to match a customer's profile. Personalization considers an individual's taste, personal preferences, demographics, and location. Offering personalized services is the best way to increase user engagement, customer satisfaction, and sales (Lalmas, 2019). Therefore, understanding customer behavior through prior interactions with the company and other companies is essential for personalization (Chellappa & Sin, 2005).

Advanced personalization capability generates value for companies and customers who benefit from an enhanced and seamless experience when dealing with a company (Hossain et al., 2020).

Most people reject personal data collection in principle; however, they expect to receive personalized services, to which they react with higher satisfaction than generic offerings (Kobsa et al., 2016). Awad and Krishnan (2006) found that consumers who were most protective of their data valued personalization the most, which they referred to as the personalization-privacy paradox.

Personalization requires people to share personal data; however, companies must comply with official privacy regulations. To improve privacy-related user experience, Wadle et al. (2019) investigated the relationship between a company's intention to disclose specific personal data categories and the type of benefit promised by personalization. They found that people were more susceptible to sharing data, such as genetic data, that pinpoint them as distinct individuals. However, people were willing to provide the same sensitive data in scenarios related to basic human needs, such as health or security.

The Economics of Privacy

The cost of storing and processing personal data has become more affordable for businesses, which allows smaller pieces of personal data to be stored, linked, and tracked to form a complete dossier of one's life. The stored profiles could contain all customer transactions performed in multiple locations, online and in real life, by the user or their household, and sometimes without the user's knowledge or consent (Lane, 2012; Yiakoumis et al., 2016). The data collection pace was accelerated for the free services.

Carrascal et al. (2013) demonstrated that free online services collect and monetize personal information, mainly via targeted advertisements. Targeted advertising is a thriving business, as the personal data value is well above the value users assign to their personal information. Users generally value their online browsing history at less than \$10 (Carrascal et al., 2013), whereas advertisers are willing to pay anything between \$15 and \$40 per user data (Kugler, 2018). The profit made from selling personal data to advertisers explains why users mostly receive targeted ads—the least preferred compensation method—despite users’ preference to exchange information for money or improved services (Carrascal et al., 2013).

Buying and selling personal data is a multibillion-dollar industry. In the United States, credit bureaus, such as Equifax, Experian, TransUnion, and data marketers and aggregators, such as Acxiom, LexisNexis, and ChoicePoint, are the leading players. These entities buy and sell data largely from retailers, banks, insurance companies, and government agencies. Nonprofit organizations also participate in privacy-related data monetization. The Center for Medicare and Medicaid Services sells individual Medicare and Medicaid claims data to insurance companies. Medicare and Medicaid claim data include medical, financial, demographic, and geographic details (Li & Raghunathan, 2014).

Cellular Service Providers

Telecom companies have abundant access to first-party data that are not available to anyone else (Ahmad et al., 2019). These companies can learn a lot from historical and real-time access to customers’ locations, activities, and habits (Bodi et al., 2010). This collection of data is a treasure for the personalization of any service. These

data can be sold to advertisers and content providers, including social media companies. Data aggregators are willing to pay high prices to access telecom companies' first-party personal data, even if anonymized (Tu et al., 2018b). Advertisers desperately need personal data to enhance their personalization and marketing campaigns to increase profits (Bharadwaj et al., 2013). Cranor et al. (2018) found that few companies disclose their data processing and retention policies. Cranor et al. (2018) and Choi et al. (2019) found that companies such as AT&T and Verizon do not disclose their practices of sharing personal information with third parties; however, these companies acknowledge the collection and processing of customers' PII (Hoa & Choub, 2014).

Despite cellular service providers being among the most qualified to have the most significant number of mobile applications users, social networks, and online advertising spaces have many more. Customers primarily use the telecom network as a pipe, often called a dumb pipe, to access internet content providers' services. Content providers, such as Google and Facebook, rely on the revenue they collect from selling targeted advertising using contextual, profile-based, behavioral, and location-based data collected from their users (Wills & Tatar, 2012). On the other hand, cellular service providers have access to data unavailable to the content providers, which could be sold to generate additional revenue to offset the decline in messaging and voice profits (Agarwal et al., 2012; Sujata et al., 2015).

Having access to nonpublic user information, regardless of user preference or consent, allows for effective targeted advertising that generates significant revenue (Wagner & Eckhoff, 2018). Cellular service providers generate additional income by utilizing the collected user data, an approach called data monetization. The data are used

to provide personalized services, offers, and content to users from third-party online advertisers (Smailovic et al., 2013). Cellular service providers collect users' internet traffic information using network intelligence and deep packet inspection (DPI) technologies. DPI provides access to a comprehensive set of data and enables the reporting of granular real-time tracking of cellular internet user traffic, behavior, and online advertising exposure. In addition, cellular service providers can use DPI to alter consumers' internet experience. For instance, AT&T sends the user to a web page full of targeted advertisements if the user has misspelled the website address they intend to visit (Hermet & Combet, 2011).

Privacy and Legal

Courts and policymakers struggled to identify the presence of privacy problems. Individuals in the legal system view privacy as a form of protection against certain harmful or problematic activities. However, the harm of violating users' privacy is not always socially undesirable or prohibited; therefore, legally addressing privacy issues can become overly complicated. Courts and lawmakers find it challenging to achieve proper assessment of harm caused by privacy violation, particularly when part of the personal information used in the violation is publicly available and no embarrassing or intimate details are exposed. Therefore, a general legal opinion exists that using personal data for commercial and marketing purposes does not constitute clear harm, especially when part of the personal data is publicly available (Solove, 2006).

Privacy Laws

The lack of a clear identification of harm caused by privacy violations has pushed countries and states to introduce privacy legislation that severely controls the

collection and processing of personal information. In Europe, the General Data Protection Regulation (GDPR) provided a precise definition for each data category and requested companies to provide clear and understandable language regarding their data collection and processing. The objective of GDPR is to obtain informed consent from customers; however, whether the information provided is transparent depends on the individual user's or data subject's cognitive abilities and language skills. Europe's GDPR is a crucial milestone in regulating customer privacy. Other governments have followed suit in creating and ratifying laws related to customer privacy. Geller (2016) classified newly established data protection regulations in South Korea and Canada as heavily regulated privacy laws, while privacy laws in the United States, Australia, New Zealand, Argentina, Japan, and Morocco were considered more lenient.

The U.S. Communications Act generally restricts telecommunication companies from collecting and disclosing customers' nonconsensual PII to third parties, except when necessary to provide service, conduct legitimate business activities related to the use, or respond to legal requests. Section 5 of the Federal Trade Commission Act provides the Federal Trade Commission (FTC) the power to prohibit unfair or deceptive acts or practices. The prohibition covers all commercial organizations that the FTC has jurisdiction over, including telecommunication companies (Culnan & Williams, 2009). In addition, leaders in individual states have exercised consumer privacy protection in their jurisdictions. The FTC and attorney general in individual states enforce transparency requirements for collecting and using PII to ensure an appropriate declaration is provided. Companies obtain consent from customers when required. For instance, on June 28, 2018, California lawmakers enacted the California Consumer

Privacy Act (CCPA), which regulates the sale of consumer information and grants California residents the ability to access and delete data related to them in certain situations. The CCPA went into effect on January 1, 2020. Other states have considered similar plans. Moreover, if passed, a federal legislative proposal will introduce new protections for consumer privacy and impose additional requirements on entities that collect and use personal consumer information. It is unclear whether this legislation is passed at the federal or state level; the impact of any such laws on telecommunication companies is unknown (California State Legislature, 2018; Comcast Corporation, 2018; Culnan & Williams, 2009).

Legislation is not the only way to preserve the privacy of data subjects. Courtesy, customs, morality, and norms often govern personal information sharing. Nissenbaum (1997) proposed implementing laws, policies, and regulations only when (a) the violations of standards are widespread and systematic, (b) strong incentives are behind these violations, or (c) the parties involved are of radically unequal power and wealth. The three conditions apply when telecommunication companies violate users' privacy. Multiple attempts have been made to implement methodologies, guidelines, and tools to aid data subjects and address the complexity and variability of privacy issues using robust and sound technological solutions (Heurix et al., 2015).

Personal Data Retention

Each transaction that goes through cellular phones leaves electronic traces, including important trails such as call details, data usage, and location data. Law enforcement agencies can use these data to investigate crimes and as evidence in court proceedings. The same data stored for a longer time can reveal individuals' life details,

social circles, movements, socioeconomic class, and habits. Storing and processing these data violates Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, which guarantees respect for private and family life (Heurix et al., 2015; Vainio & Miettinen, 2015).

It is challenging to prevent telecommunication companies from retaining or processing data, as the interest of public safety—safeguarding personal records for a potential legal request—may counter the right to privacy and the right to protect personal data. In 2014, the Court of Justice of the European Union (CJEU) ruled that the obligation imposed on public telecommunication networks to retain data related to a person's private life and their interactions *contradicts* the rights guaranteed by the Charter of Fundamental Human Rights of the European Union. Two years later, the same court ruled that member states can enforce laws that permit, as a preventive measure, the targeted retention of traffic and location data for fighting serious crime, given that the people whose data were retained have sufficient guarantees that their data will be protected against the risk of misuse. The CJEU established that access to data could only be permitted once a court decision was obtained based on the authorities' reasoned request (Vainio & Miettinen, 2015).

Privacy Violations by Telecommunication Companies

The Canadian Radio-Television and Telecommunications Commission (CRTC) and the Office of the Privacy Commissioner (OPC) of Canada have investigated Bell Sympatico's use of DPI technology to collect and use personal information from customers without consent. The OPC concluded that collecting data from customers'

internet usage without the consent of users proves that data privacy is not among the top priorities for service providers (Dowding, 2014).

Privacy Enhancing Technologies (PETs)

Individuals' perceptions and emotional reactions play a dominant role in influencing their attitudes and behaviors. Users' actions are primarily limited by their bounded logic, which prevents users from making systematic cost-benefit evaluations before making spontaneous decisions on privacy. Therefore, users need an external assistance system to make quick information disclosure decisions (Zhang & Xu, 2016).

PETs are used to protect individuals' privacy by providing anonymity, pseudonymity, and unlinkability with data subjects (Heurix et al., 2015). Wagner and Eckhoff (2018) proposed using PETs to protect privacy through system design rather than policy, which can offer much more robust protection and measure the level of system privacy or the privacy provided by a given PET. However, there has been no standard implementation or structured evaluation criteria for PETs, leading to ineffective performance. For instance, some PETs rely on anonymizing data that are easily reidentified (Ohm, 2010). Other PETs redesigned the telecommunication network architecture by encrypting, secret sharing, pseudonymizing, and anonymizing PII across all network layers. Although this approach addresses privacy issues, it creates noninteroperable networks that are not compatible with standard implementations (Yadegari & Gharaee, 2016).

Acquisti's (2009) proposal of importing the use of a soft paternal intervention from behavioral research to nudge the user toward sharing only the necessary information remains the preferred approach, as it maintains users' autonomy and ability

to make decisions. The soft paternalistic approach pushes users toward more thoughtful and informed privacy-related choices, referred to as privacy nudges. Privacy nudges can be a powerful PET mechanism to help users avoid unintended disclosures (Wang et al., 2014). Shih et al. (2015) concluded that users were more likely to share personal information when the nudges explained the request details, and users shared the most when the nudges contained vague or no information about the data being requested.

Relevant Research

Table 1 summarizes the relevant privacy studies that were reviewed to identify the research gap that this study aimed to bridge.

Table 1*Relevant Literature Review Summary*

Study	Scope	Methodology	Conclusion
Belanger & Crossler, 2019	Explored the antecedents of individuals' attitudes toward sharing information on their cellular devices, their intentions to use protective settings, and their actual practices.	Used MTurk to develop a cellular information protection model based on integrating the Theory of Planned Behavior which predicts an individual's intention to engage in a behavior at a specific time and place. Data from 228 iPhone users were tested.	Concluded that cellular information protection intentions lead to actual privacy setting practices and that attitude toward information sharing and cellular privacy protection self-efficacy affect this intention.
Balapour et al., 2020z	Applied the communication privacy management theory to mobile application users' security perceptions to examine the effectiveness of privacy policies.	Used MTurk to empirically test the proposed theoretical model and conducted two surveys using mobile applications asking for less sensitive ($n = 487$) and more sensitive information ($n = 559$).	Findings demonstrated that perceived privacy risk negatively influenced the perceived application security. The perceived effectiveness of the privacy policy positively influenced user perceptions of applications privacy awareness, and security moderated the effect of perceived privacy risk on the perceived security of mobile applications. The results suggested that users have different privacy-security perceptions based on the information sensitivity of mobile applications.

Table 1 - continued*Relevant Literature Review Summary (continued)*

von Entreß-Fürsteneck et al., 2019	Analyzed the privacy calculus influence of personal risks and benefits on the willingness to disclose personal self-tracking data to health insurance companies.	Built a conceptual model based on the privacy calculus concept and validated it ($n = 103$) in a scenario-based experiment using structural equation modeling.	Results revealed that privacy risks always harm the willingness to disclose personal data. In contrast, the positive effects of privacy benefits are partly dependent on data sensitivity.
Van Kleek et al., 2017	Examined if revealing critical data collection practices of smartphone applications may help people make more informed privacy-related decisions.	Designed Data Controller Indicators (DCIs) that exposed previously hidden information flows out of the mobile applications. A mixed-methods investigation was conducted to test data controller indicators in a realistic privacy-related decision-making setting.	Lab study results showed that out-of-flow indicators supported people in making more confident and consistent choices. Furthermore, contextualized indicators against applications already in use impacted overall information exposure.
Benndorf & Normann, 2018	Evaluated the willingness to sell personal data, such as contact information, Facebook details, and preferences.	Used laboratory experiments, using a standard incentive method to solicit personal data and provide an incentive in return. The personal data included contact details and complete Facebook profiles.	Results contradicted the hypothetical questionnaire research that found that most people would oppose selling their data in exchange for money. The incentivized study found that only 16% of people refused to sell their data, while 70% asked for an average of 15 Euros and 15% were willing to sell their data for 2.5 Euros.

Table 1 - continued*Relevant Literature Review Summary (continued)*

Study	Scope	Methodology	Conclusion
Malgieri & Custers, 2018	Analyzed if consumers should have a right to know the value of their data, based on E.U.'s legislation to protect personal data and monetization of personal data.	Quantified personal data values to demonstrate that they can be measured, which is a condition for the right to know the value of one's data.	The models were incompatible with EU data protection law. While moral problems of pricing privacy exist, they should not outweigh the benefits of introducing a right to know the value of one's data.
Mamonov & Benbunan-Fich, 2018	Examined means to protect computer users from potential security and privacy threats. Drew on the Information Processing framework, which states that threat mitigation frequently occurs before full cognitive threat assessment.	Conducted an empirical study to evaluate information security threats on the strength of passwords and the disclosure of personal information using an online experiment.	Found evidence that notifications helped reduce the disclosure of sensitive personal information and prompted users to choose 500 times stronger passwords.
Hubert et al., 2017	Investigated smartphone-based mobile shopping acceptance by examining the impact of different mobile and personal benefits (instant connectivity, contextual value, and hedonic motivation), and the perception of three mobile shopping characteristics (location sensitivity, time criticality, and extent of control).	In an empirical study on smartphone shoppers ($n = 410$), participants were invited via a survey link on an online survey platform in the UK.	Concluded that acceptance was associated with ease of use and usefulness, which drove intentional and behavioral outcomes. Risks and benefits impacted the ease of use.

Table 1 - continued*Relevant Literature Review Summary (continued)*

Study	Scope	Methodology	Conclusion
Shin et al., 2017	Examined the mechanism of notice and consent on mobile application installation.	Conducted a survey model between subject groups with different intervening messages, including notices and consent messages when installing an app.	Different messages (threat, safety, and neutral) affected installation behavior. Concluded that prior perceptions about the threat of privacy drove the awareness of notice and consent messages.
C. Robinson, 2017	Examined the effect of demographic variables on willingness to disclose and perceive PII risks on e-commerce in the United States and Estonia.	Utilized a 17-item list of potential disclosure items, such as name and email address, grouped into six subcategories (contact information, payment information, life history information, financial/medical information, work-related information, and online account information).	Americans were more willing to disclose and less concerned about perceived risks than Estonians. The findings suggested that willingness to disclose and risk aversion should be analyzed empirically together.
S. C. Robinson, 2017	Utilized communication privacy management to examine privacy concerns, such as collection, control, awareness, unauthorized secondary use, improper access, location tracking, trust in cellular advertisers, and attitudes toward cellular commerce, to predict cellular commerce engagement.	Used an online survey utilizing Qualtrics on MTurk ($n = 416$), with an HIT lasting 14 days and each participant compensated 20 cents.	Control, unauthorized access, trust in cellular advertisers, and attitude toward cellular commerce significantly predicted 43% of the cellular commerce behavior.

Table 1 - continued*Relevant Literature Review Summary (continued)*

Study	Scope	Methodology	Conclusion
Buchwald et al., 2017	Examined factors influencing willingness to disclose personal self-tracking data to service providers.	Developed a theoretical research model with no empirical examination.	As a next step, proposed to perform a survey to test the developed model using SEM.
Grabowski & Samfelt, 2016	Evaluated user awareness of data mined by mHealth companies from mobile applications and wearables usage.	Two-step face-to-face semi-structured interviews with subjects ($n = 16$) were conducted for qualitative data gathering.	Results revealed that average users did not grasp the different types of personal data that can be mined from their usage pattern. The total sample provided a comprehensive understanding. However, decisions on acting were not examined.
Leppäniemi et al., 2017	Examined the relationships among customers' willingness to share information, satisfaction, perceived value, and loyalty in a retail industry context.	Collected data from two retailing contexts: groceries ($n = 429$) and do-it-yourself ($n = 895$). Analyzed data using partial least squares structural equation modeling.	Concluded that the perceived value and satisfaction were significant determinants of customers' willingness to share information with a company.
Levin et al., 2013	Examined parents' comfort in using development sensors to record and share their domestic interactions. Levin et al., 2013.	Surveyed parents ($n = 210$) to assess their willingness to participate in various types of cellular sensor studies.	The majority (71.4%) of parents were willing to collect physical activity and vitals, such as heart rate, data. On average, 42% were willing to collect raw audio and video, but 14% were "extremely willing" to collect audio and video. Parents who owned voice-controlled speakers were more willing to collect and share data.
Limba & Šidlauskas, 2018	Investigated safe values and habits of personal data management in social networks.	Document analysis, literature review, a case study, and generalization were used.	Presented a model for user and third-party application interaction and analysis of risks and recommendations to ensure personal data security.

Table 1 - continued*Relevant Literature Review Summary (continued)*

Liu et al., 2016	The theoretical framework combined a privacy calculus model with a technology acceptance model (TAM) an information systems theory that models how users come to accept and use a technology in the mobile application context.	An incentivized study ($n = 308$) was conducted.	Concluded that perceived enjoyment replaced perceived ease-of-use as the main predictor of perceived behavioral intentions in a mobile TAM. Demonstrated that personalized services and users' perceived information control substantially affected the privacy calculus and mobile TAM.
Brandtzaeg et al., 2019	Combined individual perceptions of mobile application privacy, actual personal dataflows in applications, and their correlation to actual privacy policies and terms.	Conducted a mixed-methods study using a user survey ($n = 20$) in Norway, analyzed personal dataflows in applications, and conducted content analysis of privacy policies of 21 popular, free Android mobile applications.	Half of the respondents refrained from using applications to avoid sharing personal data. In addition, 19 of 21 applications investigated transmitted personal data to approximately 600 different primary and third-party domains, mostly in the United States.
Elvy, 2017	Examined the impact of the growing personal data economy and pay-for-privacy models.	Analyzed the pay for privacy models and practices among companies by paying customers to share their data.	Argued that pay for privacy models transform privacy into a tradable product, which may engender or worsen unequal access to privacy and enable predatory and discriminatory behavior.

Theoretical Foundation

The ELM is a persuasion theory that models how a request's characteristics influence a person's attitude formation when making a decision and their behavior toward that decision. The ELM is an invaluable theory for privacy research. It has been used to study the impact of personalized experience on customers' attitudes and

decisions. The ELM identifies two different routes to persuasion: heuristic and cognitive. Each path differs based on the level of mental effort exerted to make a decision. Low cognitive effort represents a peripheral or heuristic route to attitude formation, while high cognitive effort represents a central or cognitive route.

Zhou (2012) applied the ELM to examine customers' initial trust in mobile banking and demonstrated that both central (information quality and service quality) and peripheral (system quality, reputation, and structural assurance) cues significantly affected initial trust, with information quality, system quality, and structural assurance revealing more significant effects and self-efficacy moderating the central and peripheral routes. Bansal et al. (2008) examined privacy using the ELM and concluded that individuals with high privacy concerns trusted websites based on the central route, such as the presence and quality of privacy policies, while those with lower general privacy concerns were more influenced by peripheral cues, such as privacy seals. Joshi et al. (2016) highlighted the importance of high-speed internet access and its opportunities to develop new business models for telecommunication companies by capitalizing on the usage data they can access.

To date, research has not applied ELM to telecommunication companies. Kobsa et al. (2016) applied the ELM to the privacy versus personalization paradox and reconciled the privacy calculus view for computer users when dealing with fictitious and reputable companies such as Amazon. However, Kobsa et al. (2016) did not consider trust as a factor and included only two personal variables: privacy self-efficacy beliefs and general online privacy concerns. Similarly, Gu et al. (2017) investigated Android users' privacy concerns when downloading new smartphone applications, extending the

ELM to include the formation of users' privacy concerns as a contextual information processing outcome, with perceived application popularity as the peripheral route variable and perceived permission sensitivity and permission justification as the central route variables. Their results revealed that perceived permission sensitivity increased privacy concerns, whereas permission justification and perceived application popularity reduced privacy concerns.

Heuristic shortcuts that represent the peripheral route in the ELM have received a fair share of research. Heuristic decisions are fast decisions made when time and information are limited and often replace the rational process of making the best decisions (Acquisti & Grossklags, 2007). Quick decisions can lead to decision-making errors, mainly because of social biases. An important strategy to reduce this bias is to import the soft paternal intervention from behavioral research, namely, to nudge the user toward reducing the exposure of private information while maintaining the user's autonomy and ability to make decisions. Privacy nudges have been proposed as a mechanism to provide information to users about privacy risks. Privacy nudges encourage users to make more thoughtful and informed privacy-related decisions (Acquisti, 2009; Leon et al., 2013; Wang et al., 2014). Privacy nudges have the potential to become powerful tools to help users avoid unintentional disclosures.

The effect of deliberative cognitive processes on privacy decisions, which form the ELM's central route, has also received significant research attention. Most notably, Li and Unger (2012) found that personalization benefits could trump the impact of privacy concerns in multiple scenarios and concluded that companies could improve the perceived quality of personalization services to offset customer privacy concerns.

Chellappa and Sin (2005) found similar results and observed that the trust relationship between the consumer and the service provider positively influenced the customer's sharing behavior. This finding supports the inclusion of trust in the company in the present study.

Chapter 3

Research Methodology

Overview

This study utilized a survey instrument and a mobile application to collect the participants' responses to a questionnaire and nudges on sharing personal information with cellular service providers. The collected data were used to examine the impact of the independent variables of privacy nudges, trust level toward the company, and the amount and type of requested data on the dependent variable, personal information sharing. The ELM was used to identify the effect of peripheral versus cognitive routes on personal information-sharing behavior.

This chapter outlines the methodology for examining the drivers behind people sharing personal information with mobile network service providers. Data were collected using Qualtrics, an online survey tool. Participants who completed the survey were asked to install the Privacy Nudges mobile application to record their responses to various privacy nudges. The application presented multiple privacy nudges based on the participants' behavior. The answers were collected from the survey and application.

Research Design

This study used a quantitative approach with a post-positivist perspective, which represents a traditional form of research and is often referred to as a scientific method. This study adopted the post-positivism perspective, as it encourages further analysis of the expected positive results, challenges the absolute truth of knowledge, and recognizes

that it is nearly impossible to be certain about any theory or knowledge claim when dealing with human actions (Kobsa et al., 2016; Terrel, 2016).

The conceptual model was designed based on the ELM and existing literature. It was speculated that sharing personal information is influenced by two cognitive route constructs: the user's trust in the company, the amount and type of requested information, and a single heuristic route construct, the presence of privacy nudges. In addition, it was assumed that the influence of predictors differed between participants of different age groups. It was assumed that age moderates the influence of the three independent variables, amount and type of the requested data, user's trust toward the company, and the privacy nudges, on the dependent variable of personal information sharing.

Amazon's MTurk is an online marketplace for human tasks divided into requestors (employers) and workers, referred to as providers or turkers. When creating a new HIT, the requestor sets the price and duration expected for the job. The workers selected the task they wanted to work on for the provided pay. Participants were recruited through the Amazon Mechanical Turk (MTurk) website. MTurk and MicroWorkers are crowdsourcing job sites available on the internet, dedicated to small jobs completed in a few minutes or hours. Other crowdsourcing sites, such as Upwork, require specialized skills and longer task durations. The main benefit of MTurk to researchers is the continuously available supply of people for requested tasks, including participants for research studies, at a predefined price. Mason and Suri (2012) estimated the workers' average hourly wage between \$1.38 and \$4.80, with most workers making around \$30,000 per annum. MTurk was used to provide payouts in U.S. dollars and

Indian rupees before shifting to international payout support. Therefore, the majority of workers are residents in the U.S. or India (Mason & Suri, 2012)

The Qualtrics online survey tool was used to collect data from individuals using convenient nonprobability sampling. Inclusion criteria were (a) being 18 years of age or older, (b) using an Android smartphone with an active data plan since the mobile application was only available on Android, and (c) residing in the United States.

As the study was empirical, participants completed an online questionnaire that collected demographic information and other privacy and personalization-related data. The study instruments were submitted and exempted by the Institutional Review Board (IRB) of Nova Southeastern University (NSU). After completing the survey, participants were directed to install and use the Privacy Nudges mobile application on Google Play Store. The mobile application provided a brief introduction and asked the users to accept the experiment's terms and conditions. After installation, the application acted as if it were tracking and analyzing personal information accessed by the cellular service provider and asked participants to make decisions. The notifications alternated between asking permission to share the contact list, current location, and messages with the service provider. The application did not share any information with the researcher; participants were given the option to inspect the information that would be shared with the researcher. The application asked participants to keep running in the background to make the best use of personalized services. The application continued to send notifications based on what would be shared with the cellular service provider about the participant's location and the type of services used.

Mobile Application

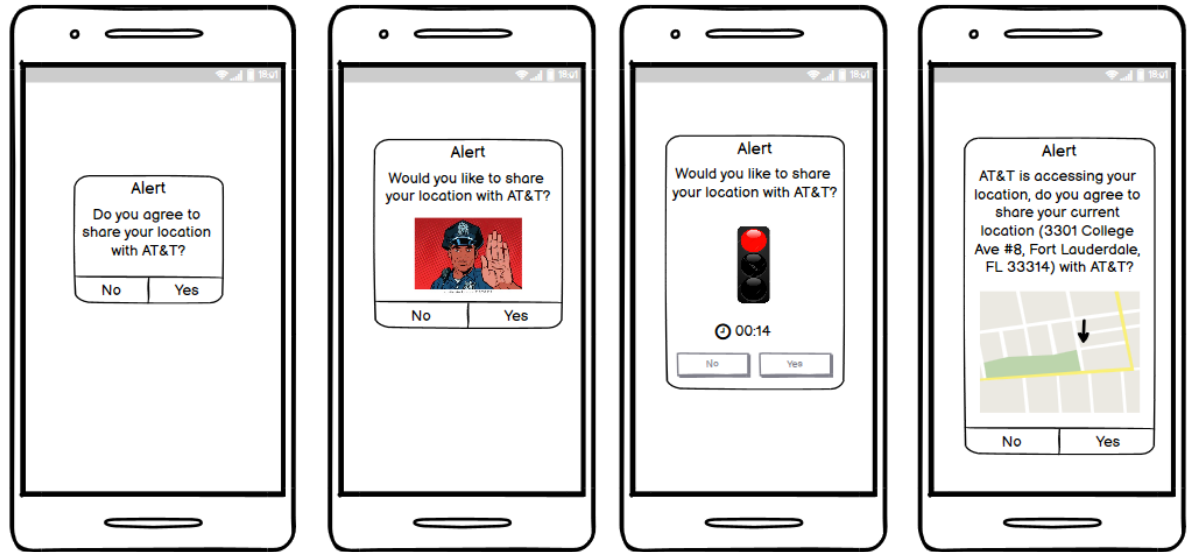
The mobile application, called Privacy Nudges, gained insight into personal information behavior and the efficacy of privacy nudges. The application was implemented on the Android platform. An iOS application was created but was rejected by Apple because of the limited number of users it targets. Participants were asked to download the application from the Google Play Store and provide the required permissions to allow the application to operate. The application collected information about the device, location, and calling events. No personally identifying information, such as name, e-mail address, or phone number, was collected. Each participant was given a unique identifier. The application created multiple types of notifications. Participants were expected to respond to the nudges when they appeared on the phone display.

The nudge design was inspired by Felt et al. (2014) and Almuhiemedi et al. (2014). The researcher communicated with Hazim Almuhiemedi regarding the proposed research design. A minimum of three different designs were implemented. Senju and Johnson (2009) found that people behaved more responsibly when an image of a face appearing to observe the user presented a warning message. Therefore, the nudge designs included human faces with eyes directed at the user, such as an icon of a criminal staring at the user or a watching policeman with his hand indicating a stop sign, called watching eye nudges. Other designs included a red traffic light with a 15-second timer, where users were asked to pause for 15 seconds and consider the consequences before deciding to share personal information. One design introduced an additional step

in which participants had to click to unfold the option of sharing before agreeing to share (Reychav & Weisberg, 2010). The nudge designs are shown in Figure 2.

Figure 2

Samples of the Nudges



The application randomly generated notifications and requested users to respond. The participants could view the log file before sharing it with the researcher. Once a nudge was displayed, the application recorded the user response and response time, which was used to identify if the response was valid, indicating whether the participant responded within a few seconds of the message or if the notification had expired by the time the user responded. Users were asked to share the log files with the researcher via the application or email at the end of the study. The study used solely the data transmitted by the participants through logfiles, with no direct information sharing to guarantee the participants' anonymity and informed data sharing.

Sampling Methods

The nonprobability sampling method was used, as not all MTurk workers had equal opportunities to participate in this study. Convenient sampling was used because of the selection of a specific target group. Judgmental and snowball sampling techniques were employed as purposive sampling to reach participants with a high engagement level, as participation required installing a mobile application on participants' smartphones.

The contribution of each of the three predictor variables to the variance of the dependent variable was investigated. Cohen's (1992) formula and G*Power 3.1 were used to calculate the based on three predictors ($u = 3$): specified power of 0.85, medium effect size f^2 of 0.15, and Cronbach's alpha (α) value of 0.05. Using a priori power analysis, the minimum sample size was determined to be 50. The calculated power of the multiple regression analysis was 0.85, which was higher than the required 0.80 (Kock & Hadaya, 2018). The sample size calculation matched the rule of thumb calculations by Kock and Hadaya (2018), who estimated that the sample size for Partial Least Square – Structural Equation Modeling (PLS-SEM) research should be at least ten times the number of constructs ($n = 50$). However, a sample size of 100 was considered ideal for this study to increase the power from $1-\beta$ to 0.986, thus increasing the credibility and validity of the findings.

Instrument Development and Validation

Data were collected using an online survey and a mobile application, which were used to test the hypotheses. Answers were rated on a seven-point Likert-type scale, which is extensively used in information system research. To further increase the

validity of the study, the usage of agree or disagree questions was limited. Höhne and Lenzner (2018) found that item-specific questions provoked higher fixation counts and higher refixing counts than agree or disagree questions. Item-specific questions utilize a seven-point, fully labeled response scale with a specific set of answers for each question, such as 1 = *very easy* to 7 *very difficult*.

The study was divided into five primary constructs that were measured and monitored: (a) the quality of privacy nudges, (b) amount and type of requested personal information, (c) trust toward the company, (d) the age group of the participant, and (e) personal information-sharing action by the participant. After adapting the instruments to suit the smartphone application context, peripheral cues were measured based on Wang et al. (2014) and Tanaiutchawoot et al. (2019). The type of requested information was based on Chellappa and Sin (2005). The amount of requested data was based on that of Li and Unger (2012). The other central cue was trust toward the company, based on Chellappa (2002, as cited in Choi et al., 2019). The potential moderating influence of age on all predictors was adapted from Bal et al. (2011; Balebako et al., 2011). A pilot test on the instruments, including the survey and the mobile application, was conducted using a sample of four, selected through convenience sampling. Participants were asked to complete the survey and install the mobile application. Few changes were made based on the feedback, mainly related to the clarity of the questions. Pilot testing ensured the reliability of the instruments before collecting the actual data. The instrument was tested for convergent and discriminant validity using exploratory factor analysis.

Survey

Qualtrics, an online survey tool, was used to collect and qualify responses. The data collected from the online survey were linked to mobile application data using the MTurk Worker ID as the identification field. The participants were sourced from MTurk, which provides access to diverse and broad participants and can be integrated with other survey management tools, such as SurveyMonkey and Qualtrics. Multiple studies have used Amazon's MTurk for privacy-related research (Aïmeur et al., 2016; Jackson & Wang, 2018; Rueben et al., 2017). Kittur et al. (2008) and Mason and Suri (2012) concluded that the results obtained from MTurk are as reliable as data that could be obtained from laboratories and other subject pools.

The survey included 40 questions, including sociodemographic information. Up to five questions were randomly asked during the survey. Participants were not allowed to return to earlier pages to check or change their answers. If the answer to the two same questions differed by more than one point, or if more than one question had different answers, the complete submission was voided. Ten items represented awareness of the amount and type of the requested information construct. The trust construct was measured using ten items. The intent to share personal information was measured using five items. The former constructs were measured using the same items in both approaches. In the second approach, actual information sharing was measured using seven items based on responses to the nudges.

Participants were asked to choose the name of their service providers from a list of 16 service providers. The service provider's name was used in the subsequent questions when referring to the service provider; for instance, if the participant chose

Verizon as their service provider, the next question was, “How familiar are you with Verizon?”

Privacy Nudges

Privacy nudge quality was the primary construct measured through the mobile application. Four types of nudges were randomly presented to the participants. Simple nudges contained only information on personal data that were requested to be shared. Watching eye nudges included the visual of a policeman who watched the participant. Timed nudges allowed the participant to respond to the request after a 15-second pause. Informed nudges presented detailed information about the request, including the potential reasons behind it (Renaud & Zimmermann, 2018).

The actual information sharing measured from the responses to the privacy nudges presented at the participant’s mobile device was measured on a binary scale. The participants were presented with five types of nudges: a nudge with the current user map, a nudge with a policeman photo asking for the location, a nudge with a policeman photo asking for the contact list, two nudges with a 15-second timer asking for the location and the contact list, and two nudges with text only asking for the location and contact list. Nudges appeared based on participants’ behavior. Each nudge asked the user to accept or decline sharing. To test the effect of the privacy nudges the hypothesis was broken down into seven sub-null hypotheses for the seven nudges. Each one was tested using the one-sample proportion tests. The sub-null hypotheses stated that the response there is no significant difference between the response to each of the nudges in other words, the probabilities of participants response to decline sharing personal information is 50%

The Awareness of the Amount and Type of the Personal Information Collection

The awareness of the amount and type of information that the service provider typically collects from customers was examined. Barth et al. (2019) classified the amount of personal information requested based on the number of permissions requested by the application and permissions based on their intrusiveness. This study followed a similar approach, differing in that the mobile application simulated information that cellular service providers would deduce from the data, as the study did not have access to the existing core network of the participants' cellular service providers. The requested data were classified as nonintrusive, slightly intrusive, intrusive, or very intrusive.

Trust Level Toward the Company

Trust plays a crucial role in people's willingness to share data with cellular service providers. People trust companies that are transparent about how consumers' personal information is being handled, as well as based on other company users (Waldman, 2016). Trust is particularly applicable to cellular service providers, as they often lack transparency regarding personal data sharing (Tu et al., 2018a). Trust involves accepting some risk when sharing data, which is compensated by the need or desire to use the service despite the potential risk (Waldman, 2016).

The Age Group of the Participant

Dowthwaite et al. (2020) found that young people are generally not aware of the possible implications of sharing personal data, including data collection, profiling, and sharing with third parties. In contrast, the older generation questioned online data-sharing practices.

Personal Information Sharing

The constructs were modified based on the Internet Users' Information Privacy Concerns (IUIPC) scale developed by Malhotra et al. (2004), which was used to measure the level of privacy concerns for the participants. This is similar to the awareness of privacy practices, as the measure in the IUIPC is awareness of privacy practices measured by the type of information requested. The intention to share personal information was included as an intermediary variable and was measured using five questions. The amount and type of information requested were recorded through privacy nudges to measure actual information-sharing behavior.

Recruitment

Participants were recruited from Amazon's MTurk, which is available to researchers and companies that use human subjects to perform HITs. The inclusion criteria were being residents of the United States, having a higher than 90% approval rate in previous tasks from other MTurk users, and having completed at least 50 tasks in the past. Participants were presented with the same questions selected randomly during the survey to ensure the validity of the submissions and prevent the robotic and random filling of data. If different answers were provided to the same question, the entire submission was rejected. The participants' compensation for completing the survey was \$2-5. Qualtrics estimated the duration to complete the survey at 9.1 minutes, setting the compensation above the federal minimum wage. The mobile application was required to run for 24 hours on the participant's phone. However, it required less than 15 minutes to respond to the generated privacy nudges. Participants were paid \$10 to \$15, which was also above the federal minimum wage.

Data Collection Procedures

Data on the present conditions at a single point in time were collected. Therefore, a cross-sectional research approach was used. A quantitative method was used for primary data collection. The researcher recorded all user inputs and provided different privacy settings, allowing different configurations to be tested when information sharing was requested.

Data Analysis Strategies

Descriptive statistics were used to portray a comprehensive image of the sample by displaying the collected data's mean, standard deviation, and score range. The application was consistent for all the participants—all participants received the same notifications. Mean values for each dimension were calculated. Partial least squares structural equation modeling (PLS-SEM) was used to provide a set of consistent and comprehensive explanations of the relationships using the data collected. PLS-SEM was selected, as it has been used in multiple privacy-related studies to assess the reliability of correlations between constructs (Chin, 1998). As a second-generation modeling technique, PLS-SEM can be used to determine measurements and structural models and to examine complicated models. In addition, PLS-SEM has minimal restrictions on sample size and measurement scales (Chin, 1998). The calculations were performed using IBM SPSS Statistics, licensed under the SPSS Grad Pack educational license, and the SmartPLS 3.1 , licensed under the monthly Pro license, and cited as required by the license agreement (Ringle et al., 2015).

The discriminant validity of the constructs was tested by calculating the average variance extracted (AVE) square root for each construct, which should be higher than

the correlations with all other constructs. Convergent validity was tested to ensure that the items adequately reflected their corresponding factors. Model reliability was verified using the composite factor reliability (CFR) and Cronbach's alpha (α), where both values should be 0.7. Model fit was confirmed using two measures for absolute fit, such as root-mean-square error (RMR) and Chi-Square, and comparative fit, such as the comparative fit index (CFI) and normed fit index (NFI).

Resource Requirements

A mobile application for custom-built privacy nudges was built using Android Studio. Google Cloud Platform was used for backend application development.

Summary

This chapter provided an overview of the research methodology, data analysis, and reporting tactics. Before commencing the data collection, IRB approval was obtained based on the research proposal, which included the survey and mobile application tools. The sources from which the study and application designs were adapted were detailed. Participants were sourced from MTurk; each participant had to consent before answering the survey. Another consent screen was also present on the mobile application, and participants had the choice to withdraw at any time. No personal data were collected from the survey nor the mobile application. This study aimed to help users make better privacy decisions by understanding the factors that affect the sharing of personal information with their cellular service providers.

Chapter 4

Results

Overview

This chapter provides the data analysis outcomes generated from the responses to the privacy mobile application and survey, including the sample description, construct reliability, and hypothesis testing.

Data Collection

First Approach

The survey was distributed through MTurk. Once completed, the survey displayed a code that the participants needed to use in the mobile application. The privacy nudges application was downloadable from the Android Play Store. The application would start if a valid code was entered see Figure 3. The survey completion code linked survey responses and responses from the application. Participants were paid \$5 to complete the survey, and \$10 to install the mobile application and run it for 24 hours. From the first batch of 100 participants who completed the survey, only 10 participants installed the application on their mobile phones, and only six kept it running for 24 hours. The process flow was tested multiple times to eliminate any technical issues. The only identified constraint was that the application was only available for Android phones. Android users represented approximately 67% of the total number of participants. Therefore, creating an iOS application was deemed necessary.

The application was rebuilt using the Google Cloud Platform and Flutter/Dart as a programming language to support iOS and Android devices. Unfortunately, the

submission of the iOS application was rejected by Apple due to terms and conditions regarding limited functionality. Web applications could not be used for this study because they lack the ability to provide nudges, which is an essential part of this study. Therefore, an iOS application could not be made available.

Despite multiple attempts using the Android application, of 539 completed surveys, only 29 participants installed the mobile application, and only 11 kept it running. Therefore, another approach was attempted to increase mobile application participation. MTurk allows the requester to pay a bonus to workers who exhibit extra effort. A batch targeting 500 participants was created, which paid \$2 for survey completion and \$10 for completing the mobile application component. This required extensive manual checking and verification of each participant to ensure that the bonus was paid fairly. However, this process only increased the number of mobile application users to 34, while the number of survey participants increased dramatically to 916. Therefore, optimization of the process was required, focusing on the mobile application rather than the survey.

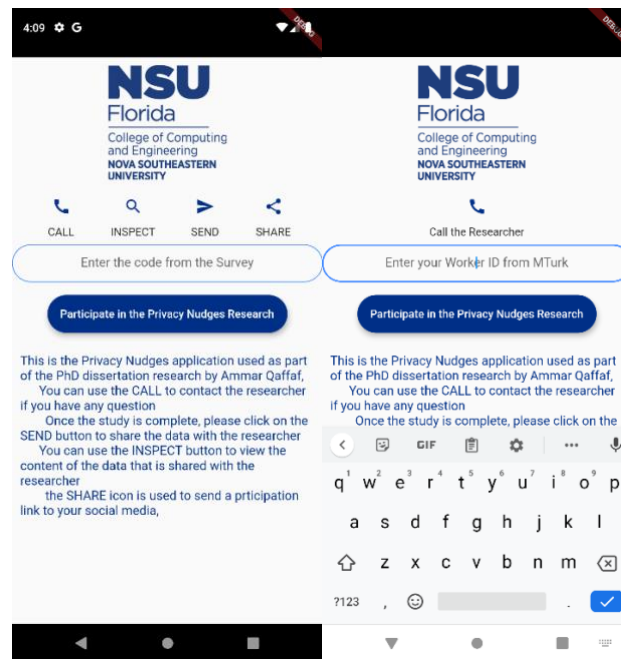
Second Approach

Each MTurk worker has a unique 10-digit code, called the MTurk ID or worker ID. Participants were first requested to install the mobile application, rather than filling the survey. Those who successfully installed the application and kept it running were asked to complete the survey. The new application required participants to enter their unique 10-digit Mturk ID instead of the survey completion code see Figure 3, which allowed any MTurk worker to participate without prior approval by the researcher or

completing the survey. In addition, the 24-hour requirement was relaxed to four hours, provided the participants answered all the nudges they received.

Figure 3

Android Mobile Application Home Page (First and Second Approaches)



The new process yielded 125 participants who installed the application, of which 118 kept the application running for four hours as requested and completed the survey, achieving a sample size of 118, which was above the target sample size of 100 and more than the 80 participants recommended by Kock and Hadaya (2018).

Data Screening

Sociodemographic data from both surveys were analyzed to ensure that a representative number of participants was captured in the survey. Data were analyzed for missing data and outliers to ensure their suitability for analysis. Multiple methods were used to ensure the quality of the data collected from MTurk. Buchanan and

Scofield (2018) detailed multiple screening steps to confirm the reliability of responses when using MTurk, including page submission time, number of options used, and bot detection. Page submission time and the number of options used were recorded through the MTurk quality check before accepting the responses and including them in the survey. Bot detection was performed using the Qualtrics captcha option, which prevents any automated bot from completing the survey. Additional fraud-detection methods were utilized, including the Qualtrics ReleventID multiple submission detection feature, which prevents the same user from submitting multiple submissions.

Demographic Analysis

Of the 916 survey submissions obtained from the first approach, 791 passed quality checks. With the second approach, 118 participants installed the mobile application, kept it running as requested, and completed the survey, the data used for the hypothesis testing relied mainly on the participants who installed the mobile application.

As detailed in Table 2 below, of the 791 participants, 77.4% were men, and 22.6% were women. The survey asked for the birth year of the participant, which allowed for greater granularity in calculating age since age was a moderating variable. Approximately half of the participants (49%) were younger than 35 years of age. The age groups included 40 (5.1%) participants between 18 and 25, 347 (43.9%) participants in the 26–35 age group, 219 (27.7%) participants in the 36–45 age group, 132 (16.7%) between 46 and 55 years of age, 42 (5.3%) participants between 56 and 65 years of age, and 11 participants older than 65 years. The majority of the participants ($n = 691$, 87.4%) were Caucasian, 63 (8.0%) were Black or African American, 20 (2.5%) were Asian, eight (1.0%) were American Indian or Alaska Native, two (0.4%) were Native

Hawaiian or Pacific Islanders, five (0.6%) identified themselves as other ethnicities, and five (0.5%) preferred not to respond to this question. Most of the participants ($n = 453$, 57.3%) had a 4-year bachelor's degree, 218 (27.6%) had a master's degree, and nine (1.1%) had a doctoral degree. In addition, 32 (4.0%) had an associate degree, and 40 (5.1%) had some college education with no degree. Furthermore, 129 (16.3%) participants had an income level between \$50,000 and \$59,999, 330 (41.7%) participants had an income below \$40,000, 332 (42.0%) participants had an income of \$60,000 or more, and 414 (52.3%) participants had an income level between \$40,000 and \$79,999.

Of the 118 participants obtained using the second approach, 72 (61.0%) were male and 46 (39.0%) were female, and 92 (78.0%) identified themselves as Caucasian, 17 (14.4%) were Black or African Americans, four (3.4%) were Asians, and two (1.7%) were other ethnic groups. The majority ($n = 67$, 56.8%) were in the 26–35 age group, followed by the 46–55 age group ($n = 22$, 18.6%) and the 18–25 age group ($n = 7$, 5.9%). None of the participants were above 61 years of age.

Table 2

Sociodemographic Characteristics of Survey Participants

Characteristics	First Approach ($n = 791$)		Second Approach ($n = 118$)	
	N	%	n	%
Age Group				
Less than 18	0	0.0	0	0.0
18 – 25	40	5.1	7	5.9
26 – 35	347	43.9	67	56.8
36 – 45	219	27.7	22	18.6

Table 2 - continued*Sociodemographic Characteristics of Survey Participants*

Characteristics	First Approach (<i>n</i> = 791)		Second Approach (<i>n</i> = 118)	
	N	%	n	%
46 – 55	132	16.7	13	11.0
56 – 65	42	5.3	9	7.6
66 or older	11	1.4	0	0.0
Gender				
Male	519	65.6	72	61.0
Female	270	34.1	46	39.0
Non-binary	0	0.0	0	0.0
Prefer not to respond	2	0.3	0	0.0
Ethnicity				
Caucasian	691	87.4	92	78.0
Black or African American	63	8.0	17	14.4
American Indian or Alaska Native	8	1.0	3	2.5
Asian	20	2.5	4	3.4
Native Hawaiian or Pacific Islander	0	0.0	0	0.0
Other	5	0.6	2	1.7
Prefer not to respond	4	0.5	0	0.0
Highest education				
Less than a high school degree	1	0.1	2	1.7
High school graduate (high school diploma or equivalent, including GED)	36	4.6	5	4.2
Some college with no degree	40	5.1	7	5.9
Associate degree (2-year)	32	4.0	4	3.4
Bachelor's degree (4-year)	453	57.3	71	60.2
Master's degree	218	27.6	28	23.7
Doctoral degree	9	1.1	0	0.0
Professional degree (JD, MD)	2	0.3	1	0.8

Table 2 - continued*Sociodemographic Characteristics of Survey Participants*

Characteristics	First Approach (<i>n</i> = 791)		Second Approach (<i>n</i> = 118)	
	N	%	n	%
Income level				
Less than \$10,000	18	2.3	2	1.7
\$10,000 to \$19,999	53	6.7	4	3.4
\$20,000 to \$29,999	68	8.6	16	13.6
\$30,000 to \$39,999	65	8.2	17	14.4
\$40,000 to \$49,999	126	15.9	13	11.0
\$50,000 to \$59,999	129	16.3	31	26.3
\$60,000 to \$69,999	62	7.8	12	10.2
\$70,000 to \$79,999	97	12.3	9	7.6
\$80,000 to \$89,999	39	4.9	6	5.1
\$90,000 to \$99,999	57	7.2	3	2.5
\$100,000 to \$149,999	58	7.3	5	4.2
\$150,000 or more	19	2.4	2	1.7
Prefer not to respond	0	0.0	0	0.0

In the first approach as detailed in Table 3 below, AT&T was the carrier with the most significant number of customers (21.1%), followed by T-Mobile (19.0%), Verizon (18.8%), and Google Fi (15.5%). In the second approach, Google Fi came first, with almost a quarter of the participants using it (25.4%), followed by T-Mobile (24.6%), Verizon (15.3%), and AT&T (10.2%). Participants in both approaches were heavy smartphone users, with 43.5% and 49.2% using their phones 4 to 6 hours daily in the first and second approaches, respectively.

Table 3*Cellular Phone Service Characteristics*

Characteristics	First Approach (<i>n</i> = 791)		Second Approach (<i>n</i> = 118)	
	<i>n</i>	%	<i>n</i>	%
Wireless Service Provider				
AT&T	167	21.1	12	10.2
Verizon	149	18.8	18	15.3
T-Mobile	150	19.0	29	24.6
Sprint	32	4.0	9	7.6
Virgin Mobile	31	3.9	1	0.8
Boost	29	3.7	3	2.5
Mint	14	1.8	0	0.0
Google Fi	123	15.5	30	25.4
Visible	2	0.3	1	0.8
US Cellular	34	4.3	7	5.9
Cricket	18	2.3	2	1.7
Metro	4	0.5	1	0.8
Straight Talk	13	1.6	2	1.7
Lyca	4	0.5	1	0.8
Ting	3	0.4	0	0.0
Other	18	2.3	2	1.7
Smartphone operating system				
iOS (Apple)	179	22.6	0	0.0
Android (Samsung, Google, Motorola, etc.)	612	77.4	118	100
Other (Windows, Blackberry, etc.)	0	0.0	0	0.0
Daily smartphone usage				
Less than 1 hour	41	5.2	3	2.5
1 - 3 hours	237	30.0	37	31.4
4 - 6 hours	344	43.5	58	49.2
7 - 10 hours	119	15.0	14	11.9
More than 10 hours	50	6.3	6	5.1

Survey

Reliability of the Constructs

SmartPLS 3.1 and IBM SPSS Statistics Version 28 were used to calculate the construct's reliability. Cronbach's alpha, composite reliability, and internal reliability assessment coefficient (Rho A) were used to measure the reliability of the constructs. In the first approach, as shown in Table 4 below, the Cronbach's alpha of the awareness of the amount and type of information sharing was 0.733, and the consistent reliability Rho A (ρ_A) was 0.866, both above the 0.7 accepted values for reliability. Cronbach's alpha for the intent to share personal information was 0.723, and Rho A 0.748, which were above 0.7. The trust construct had a Cronbach's alpha of 0.875 and Rho A of 0.900, making it the most reliable construct in this study. The moderating variables were above the 0.7 thresholds, except for age moderating awareness, which was 0.655. However, according to Ab Hamid et al. (2017), "values of composite reliability/Cronbach alpha between 0.60 and 0.70 are acceptable" (p. 2).

Table 4

Construct Reliability: First Approach (n = 791)

	Cronbach's α	ρ_A	Composite Reliability
Age moderating awareness	0.706	1.000	0.655
Age moderating trust	0.881	1.000	0.895
Awareness	0.733	0.866	0.834
Intent to share	0.723	0.748	0.816
Trust	0.875	0.900	0.899

In the second approach, as detailed in Table 5 below, Cronbach's alpha value for the awareness of the amount and type of information-sharing construct was 0.783, which

was above the generally accepted 0.7 value. The composite reliability was 0.848, and the Rho A value of 0.790 confirmed the reliability of the construct used to build the model. The trust construct also achieved an acceptable Cronbach's alpha value of 0.822, Rho A of 0.849, and a composite reliability value of 0.873, confirming the validity of the construct. The intent to share behavior had Cronbach's alpha, Rho A, and composite reliability values of 0.710, 0.768, and 0.820, respectively. Age was presented in seven groups as a moderating variable. Both age-moderating awareness and age-moderating trust achieved Cronbach's alpha values above 0.7. The Cronbach's alpha of the nudge construct was 0.801, Rho A was 0.863, and composite reliability was 0.820.

Table 5

Construct Reliability and Validity: Second Approach (n = 118)

	Cronbach's α	ρ_A	Composite Reliability
Actual sharing (response to the nudge)	0.865	0.886	0.895
Age moderating awareness	0.801	1.000	0.774
Age moderating trust	0.940	1.000	0.948
Awareness of privacy practices	0.785	0.780	0.830
Intent to share	0.799	0.802	0.861
Trusting the service provider	0.908	0.860	0.913

Another approach to verifying the constructs' validity was to evaluate the discriminant validity by calculating the heterotrait-monotrait ratio of correlations (HTMT), which refers to the extent to which the construct is empirically different from one another and the degree of differences between overlapping constructs. If the HTMT value was below 0.85, discriminant validity was established (Ab Hamid et al., 2017; Yusoff et al., 2020). All constructs were valid based on the HTMT, as detailed in Table 6 below.

Table 6*Heterotrait-Monotrait (HTMT) Ratio of Correlations*

	Actual sharing (response to the nudge)	Age group	Age moderating awareness	Age moderating trust	Awareness of privacy practices	Intent to share
Actual sharing (response to the nudge)						
Age group	0.065					
Age moderating awareness	0.186	0.207				
Age moderating trust	0.101	0.124	0.602			
Awareness of privacy practices	0.182	0.107	0.281	0.205		
Intent to share	0.235	0.036	0.216	0.166	0.614	
Trusting the service provider	0.133	0.138	0.247	0.408	0.657	0.180

For the H1 hypothesis, the one-sample proportions procedure test provided tests and confidence intervals for individual binomial proportions. Each nudge is assumed to form a different null hypothesis and is tested as a separate respective interval based on the binomial proportion. The analysis in Table 7 includes the observed proportion, the estimate of the difference between the population proportion and the hypothesized proportion. The analysis was performed using the standard Wald and Clopper-Pearson test at a 95% confidence level as detailed in Table 7 below.

Table 7*One-Sample Proportions Confidence Intervals*

Interval Type		Observed			Asymptotic Standard Error	95% Confidence Interval	
		Successes	Trials	Proportion		Lower	Upper
Nudge with map asking for location = Decline	Clopper- Pearson ("Exact") Wald	57	118	0.483	0.046	0.390	0.577
Nudge with police asking for contacts list = Decline	Clopper- Pearson ("Exact") Wald	44	118	0.373	0.045	0.286	0.467
Nudge with police asking for location = Decline	Clopper- Pearson ("Exact") Wald	52	118	0.441	0.046	0.349	0.535
Nudge with timer asking for contacts list = Decline	Clopper- Pearson ("Exact") Wald	50	118	0.424	0.045	0.333	0.518
Nudge with timer asking for location = Decline	Clopper- Pearson ("Exact") Wald	57	118	0.483	0.046	0.390	0.577
Nudge with text asking for contacts list = Decline	Clopper- Pearson ("Exact") Wald	40	118	0.339	0.044	0.254	0.432
Nudge with text asking for location = Decline	Clopper- Pearson ("Exact") Wald	51	118	0.432	0.046	0.341	0.527
		51	118	0.432	0.046	0.343	0.522

Findings

The hypotheses were divided into the two elaboration likelihood model (ELM) decision-making routes, the peripheral and central routes. The peripheral study findings

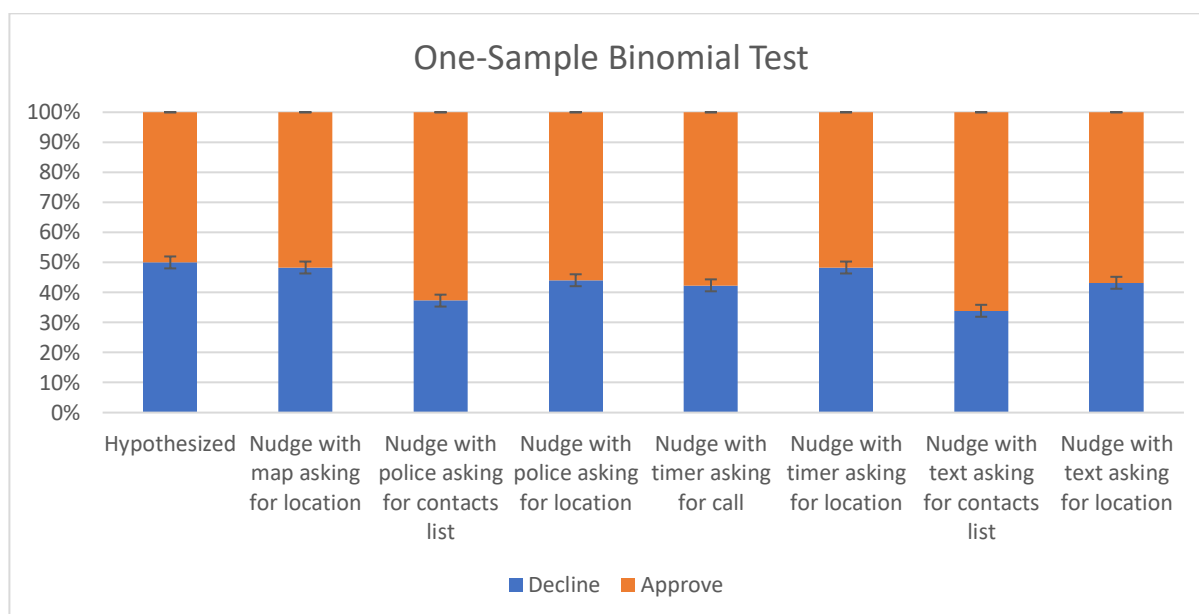
were based on data collected from the second approach, which included the mobile application and the survey.

Peripheral Hypothesis Testing

The peripheral and heuristic routes proposed by the ELM were measured to test hypothesis H1 (more informed privacy nudges negatively influence customer choices to share personal information with the cellular service provider) and H4 (Age moderates the effect of privacy nudges on information sharing).

Figure 4

One-Sample Binomial Test for the nudges and the hypothesized percentages



The H1 hypothesis was examined by breaking it down into seven null hypotheses, one for each nudge, and testing them using the binomial test, see Figure 4 above. The binomial test, also known as the test of one proportion, can be used since the response of the nudges represent a dichotomous response variable where the reactions are either accept or decline the information sharing with the service provider, as depicted in Figure 4 above. For the hypotheses testing we assumed the decline response

as the “success” of the test and the accept response as “failure” since accepting the information sharing is the default action if the user did not response to the nudge. It was hypothesized that each nudge will result in a 50% decline (p -value =.5) response to the information sharing and corresponding 95% confidence interval (CI).

Table 8

Hypothesis Test Using One-Sample Binomial Test

No.	Null Hypothesis	Sig.	Decision
1	The response to the nudge with a map asking for location = Decline occurs with a probability of 0.50.	0.782	Retain the null hypothesis.
2	The response to the nudge with police asking for contacts list = Decline occurs with a probability of 0.50.	0.008	Reject the null hypothesis.
3	The response to the nudge with police asking for location = Decline occurs with a probability of 0.50.	0.231	Retain the null hypothesis.
4	The response to the nudge with timer asking for contacts list = Decline occur with a probability of 0.50.	0.118	Retain the null hypothesis.
5	The response to the nudge with the timer asking for location = Decline occurs with a probability of 0.50.	0.782	Retain the null hypothesis.
6	The response to the nudge with text asking for contacts list = Decline occurs with a probability of 0.50.	0.001	Reject the null hypothesis.
7	The response to the nudge with text asking for location = Decline occurs with a probability of 0.50.	0.167	Retain the null hypothesis.

Results in Figure 4 and Table 8 indicate a statistically significant effect of the nudge with police asking for the contact list. Therefore we reject the null hypothesis, that the probability of rejecting sharing personal information is 50%, and accept the alternative hypothesis that the nudge with a police photo asking for the participant's contacts list positively affects sharing personal data with the service provider. Similarly,

the nudge with text asking for the contact list shows a statistically significant effect on sharing personal information. Therefore we also reject the sub-null hypothesis that the nudge with text asking for the contacts list has no significant effect on declining sharing personal data with the service provider and accept the alternative hypothesis that the nudge with text asking for the contact list positively affect sharing data. The significance for the other five nudges; nudge with a map asking for the location, nudge with police asking for the location, nudge with a timer asking for the location, and the nudge with text asking for location are not statistically significant, which indicates strong evidence for the sub-null hypothesis. Therefore, we retain the null hypothesis and fail to reject them.

Since the results of the five sub-null hypotheses had no statistically significant effect on sharing personal information, the two sub-null hypotheses that had statistical significance had a positive effect on sharing personal data. As such, the first hypothesis cannot be supported. The no significant impact of privacy nudges on sharing personal information could be attributed to multiple reasons: (a) participants knew their service provider already have access to their data. They, therefore, were less concerned about sharing the same information again. (b) participants wanted to use their phone at the time of the nudge and were concerned that rejecting to share such information could affect the rendering of the service, or just wanted to dismiss the nudge, so they chose randomly any option. (c) similar to Johnson (2012), who found no statistical significance across all conditions for Facebook privacy settings, they justified their findings by concluding that users' privacy decisions do not reflect their sharing intentions.

The corollary to the usage of nudges is that the participants, on average, rejected to share their personal information 42.5% of the time across all the nudge types, as reported in Table 9. Of the requests to share the participants' location, 48.3% declined the request when it contained a map with the location or a 15-seconds timer. In comparison, nudges requesting access to the contacts list with text-only were declined 33.9% of the time, suggesting that location information could be more personal than the contact list from the participant's perspective

Table 9

Decline and Approval Percentage of Privacy Nudges

	Declined (%)	Approved (%)
Nudge with a map asking for the location	48.3	51.7
Nudge with timer asking for the location	48.3	51.7
Nudge with police asking for the location	44.1	55.9
Nudge with text asking for the location	43.2	56.8
Nudge with timer asking for the contact list	42.4	57.6
Nudge with police asking for the contact list	37.3	62.7
Nudge with text asking for the contact list	33.9	66.1

The fourth hypothesis tested if age moderates the effect of privacy nudges on information sharing. Hierarchical regression was used to test H4. The results are presented in Table 10.

Table 10*Mann-Whitney Ranks for the Age Groups and Nudges*

	Age Group	N	Mean Rank	Sum of Ranks
Nudge with a map asking for the location	Below or equal to 40	87	62.23	5414
	Older than 40	31	51.84	1607
	Total	118		
Nudge with police asking for the contacts list	Below or equal to 40	87	61.83	5379.5
	Older than 40	31	52.95	1641.5
	Total	118		
Nudge with police asking for the location	Below or equal to 40	87	57.02	4960.5
	Older than 40	31	66.47	2060.5
	Total	118		
Nudge with a timer asking for the contacts list	Below or equal to 40	87	62.12	5404.5
	Older than 40	31	52.15	1616.5
	Total	118		
Nudge with timer asking for the location	Below or equal to 40	87	60.87	5296
	Older than 40	31	55.65	1725
	Total	118		
Nudge with text asking for the contacts list	Below or equal to 40	87	59.83	5205.5
	Older than 40	31	58.56	1815.5
	Total	118		
Nudge with text asking for the location	Below or equal to 40	87	59.91	5212
	Older than 40	31	58.35	1809
	Total	118		

Table 10 shows the results of the Mann-Whitney U test for testing the effect of the age group (below or equal to 40 years and below 40 years of age) on the nudge response. The Mann-Whitney U test was used to see if individuals differed based on their age group on answering a nudge to share personal data. The results revealed no statistically significant impact on the dependent variables see Table 11. The results do not support the fourth hypothesis, showing there is no effect for the age group on the response of the privacy nudges.

Table 11*Mann-Whitney U Test of the Moderating Role of Age: Fourth Hypothesis*

	Nudge with map asking for location	Nudge with police asking for contacts list	Nudge with police asking for location	Nudge with timer asking for call	Nudge with timer asking for location	Nudge with text asking for contacts list	Nudge with text asking for location
Mann-Whitney U	1111	1146	1133	1121	1229	1320	1313
Wilcoxon W	1607	1642	4961	1617	1725	1816	1809
Z	-1.678	-1.482	-1.536	-1.629	-0.844	-0.216	-0.253
Asymp. Sig. (2-tailed)	0.093	0.138	0.125	0.103	0.399	0.829	0.800
Exact Sig. (2-tailed)	0.100	0.194	0.144	0.138	0.412	1.000	0.835
Exact Sig. (1-tailed)	0.070	0.102	0.091	0.078	0.262	0.497	0.481
Point Probability	0.041	0.057	0.052	0.045	0.116	0.169	0.161

Cognitive Hypotheses Testing

The study focused on sharing personal information with wireless service providers, including intent to share and actual information-sharing actions in response to the privacy nudge. This study focused on the effect of the trust relationship with the service provider and awareness of the amount and type of collected data on participants' privacy decisions. The moderating effect of age on independent variables was examined. Five cognitive hypotheses were tested as detailed in Table 12 below

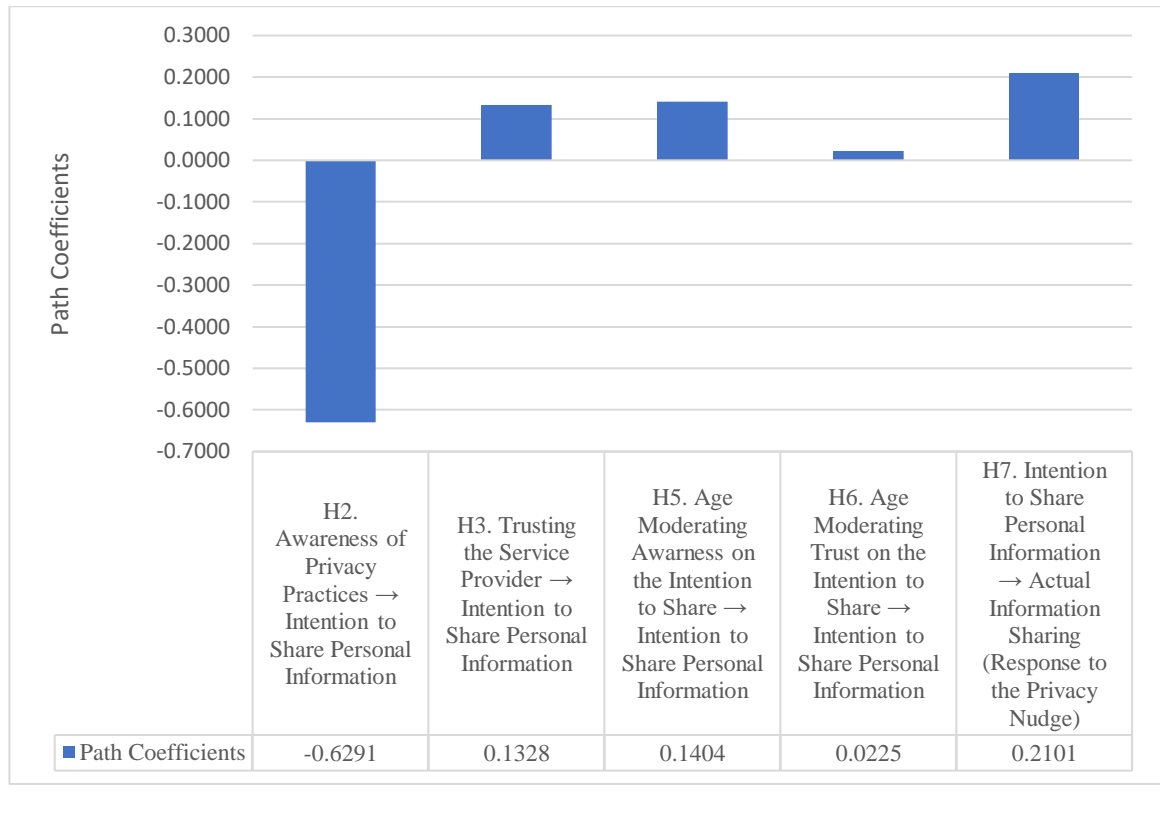
Table 12*Path Coefficients: Second Approach (n = 118)*

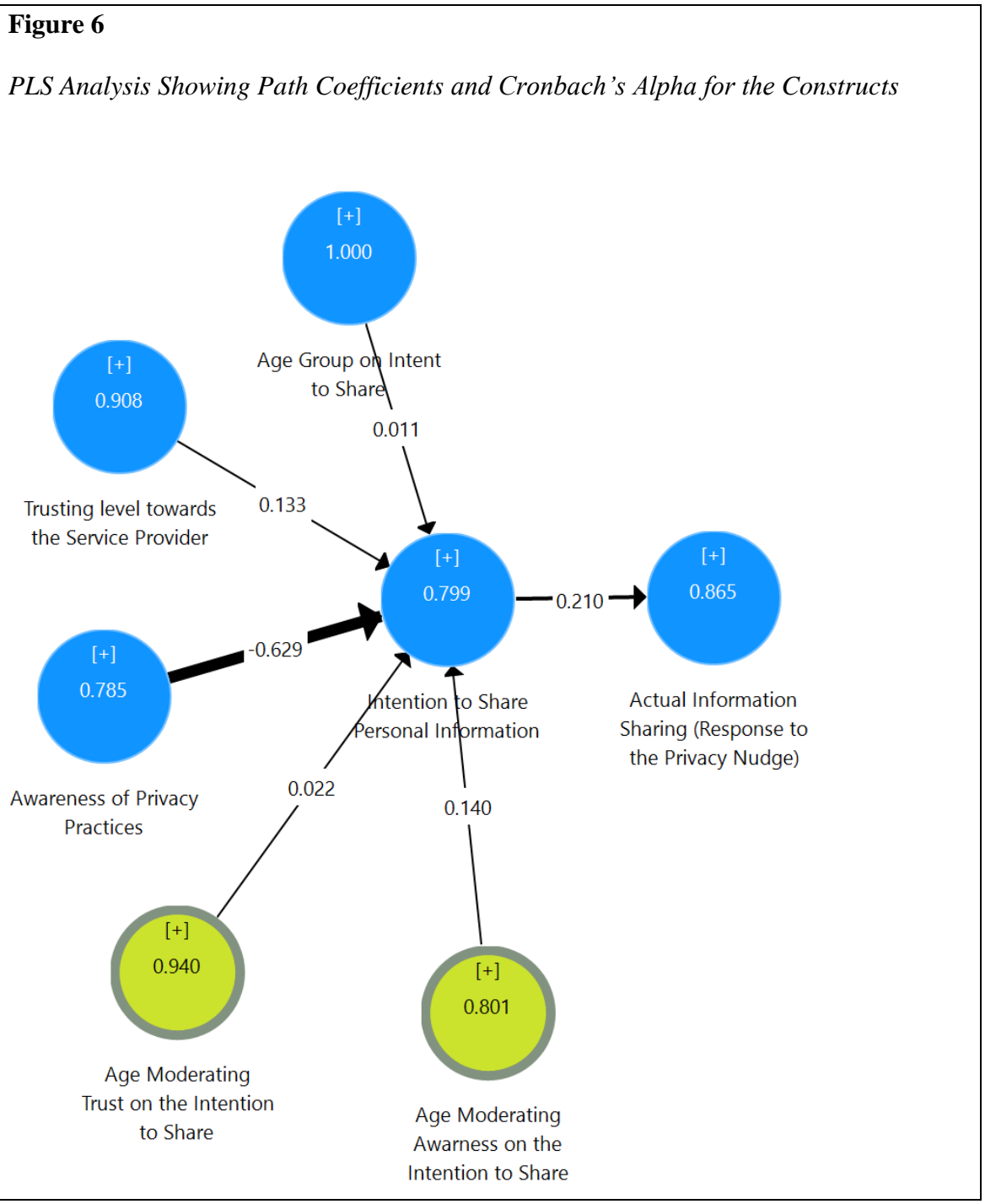
	Path Coefficient	<i>t</i> Value	<i>p</i> Values	Result
H2. Awareness of privacy practices → Intent to share personal information	-0.629	6.606	0.001	Supported
H7. Intent to share personal information → Actual information sharing (response to the privacy nudge)	0.210	2.288	0.022	Supported
H3. Trusting the service provider → Intent to share personal information	0.133	1.000	0.317	Not Supported
H5. Age moderating awareness → Intent to share personal information	0.140	0.974	0.330	Not Supported
H6. Age moderating trust → Intent to share personal information	0.022	0.188	0.851	Not Supported

Figure 5 and Figure 6 below show that the awareness of the amount and type of collected data by service providers was negatively influenced by the intent to share personal information with the service provider, supporting the second hypothesis ($\beta = -0.629$; $p = 0.001$). The seventh hypothesis that customers are more likely to reject actual data with companies when they intend not to share personal data was also supported ($\beta = 0.210$; $p = 0.022$). The third hypothesis was not supported, which stated that a higher level of trust toward the cellular service provider is associated with a higher intention to share personal information ($\beta = 0.132$; $p = 0.3345$). The fifth hypothesis that the age group moderates the effect of awareness on information-sharing intention was not supported ($\beta = 0.140$; $p = 0.330$). Likewise, the sixth hypothesis that the age group moderates the effect of trust on the intention to share personal information was not supported ($\beta = 0.022$; $p = 0.851$).

Figure 5

Path Coefficients (n=118)





Summary

This chapter presented the findings and their interpretations. Two studies were conducted: one using a survey without a mobile application with 791 participants and a

study with 118 participants who completed the survey and the mobile application installation and usage. IBM SPSS was used for collecting, cleansing, and formatting the data. SmartPLS 3 was used to analyze the data using both the PLS algorithm and bootstrapping calculations. Seven hypotheses were presented in this study, grouped into two decision-making routes based on ELM; the cognitive route was represented by H2, H3, H5, and H6, and the peripheral decision-making represented by H1, H4, and H7. The results showed that two hypotheses were supported (H2 and H7), while the other hypotheses (H1, H3, H4, H5, and H6) were found not to have a significant effect on personal information sharing and, hence, not supported.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

Conclusions

It is commonly believed that privacy is overstated, people do not care about privacy, and they avoid reading privacy policies (Acquisti et al., 2017). In addition, it has been debated whether there is a discrepancy between people's stated privacy preferences and actual behavior (Almuhimedi, 2017). However, this research found otherwise. The findings of this research suggest a positive contribution to the intention to share personal information on the actual sharing of information. People who stated their intent not to share their personal information did not share them when they were given a choice (Alemany et al., 2019).

The study aimed to reconcile rational privacy calculus and heuristic decisional shortcuts when sharing personal information with cellular service providers. The heuristic decisional route was measured using privacy nudges on an Android application to investigate actual responses to real-time privacy nudges.

The research question of this study was concerned with determining the factors that influence users' decisions to share personal information with their cellular service provider. The studied factors included awareness of the amount and type of personal information collected by service providers. A practice employed unilaterally to collect data on billions of customers by almost all companies (Christl, 2017), including 95% of the Fortune 500 companies (Case & King, 2021), and has increased during the COVID-19 pandemic (Fahey & Hino, 2020). This research suggests that 16.9% of the

participants were not aware of the practices used by their service providers to access their personal information. These findings align with those of Falivene (2021), who found that 25% disregarded the exposure of their personal information. Not everyone knows the extent of the data collection practices by companies, and “most companies are silent with regard to important consumer-relevant practices including the collection and use of sensitive information”(Cranor et al., 2018, p. 11). Knowing about these practices and the extent of personal data collection has a clear impact on the user’s decision to share their data. The oblivious person could opt to share more data as a precaution not to lose some of the benefits they expect to receive, whether the requested data are sensitive or genuinely needed to receive the benefit. Personalized promotions have positively increased the self-disclosure of personal data (Zeng et al., 2020). Users avoided disclosing their financial information for fear of being audited by the authorities (Willis, 2013). In other words, people worry about the extent to which the disclosure of this information can expose them to public oversight and the actions that can then be taken against them, yet are willing to share to gain benefits (Pitkänen & Tuunainen, 2012).

Age plays a vital role in privacy literature. Huberman et al.(2005) found that young people are more willing to share personal information than older people. However, in this study, age did not significantly affect any independent variables. Surprisingly, trusting the service provider did not significantly influence the sharing of personal data. Most participants trusted their service providers, while only 7.6% thought their service provider was not trustworthy. However, even though people trust their service provider and have established a commercial agreement by being their customers,

they still demand a level of control over what personal information is shared (Chellappa, 2002). Trust is one of the main factors affecting the relationship between a company and customer. Once trust is established, customers find it easier to share data, knowing their information is safeguarded, will not be exploited, and will only be used to improve service quality, personalized promotions, and rewards (Aimeur, 2018; Casadesus-Masanell & Hervás-Drane, 2020). This research finding contradicts the findings of Paramarta et al. (2019), who found that user awareness and trust have a positive and significant effect on sharing personal data on social media. The contradiction could be attributed to the participants' age difference in both studies; in Parmarta's study, 63.9% of participants were below 30 years old, compared to 27.9% in this research. Their research was conducted in Jakarta, Indonesia, which might also impact trust due to cultural differences (C. Zhao et al., 2012). In addition, this study contradicts the findings of Thi et al. (2020), who found a significant positive relationship between trust and the decision to share information on websites; their research was also limited to students in Hanoi, Vietnam, where cultural differences could have an influence (C. Zhao et al., 2012).

Perhaps the most important finding from this study is that people care about their privacy. When participants were given a choice to decline sharing information with their service provider, an option not available to most people, 42.5% of the requests to share personal information were declined. Declining to share personal information suggests that the intention to protect personal information may translate into action if users can choose. It was found that the design of the nudge had no significant influence on the decision to share information, whether the nudge had a detailed explanation, with

graphics, or just a bare nudge. The nudge design had no effect when people just wanted to dismiss the nudge because they thought it was unimportant or it obstructed what they were doing at the time. This could also be related to the absence of information about the risks of disclosing information, leading to poor user assessments, so these nudges are not sufficiently taken care of and knowing the risks of disclosing information, thus undermining the privacy behavior of users. This result agrees with the findings of Bergram et al.'s (2020) study, which showed that users tend to agree without ever viewing or reading the digital nudges. In addition, the findings agree with the study of Barev et al. (2021), which indicated that privacy nudges negatively influence information disclosure behavior. Barev found that some people considered nudges as a threat and that “privacy social nudge does not directly influence the intention to disclose personal information” (Barev et al., 2021, p. 4121). On the other hand, this result did not agree with the findings of Zhang and Xu (2016). They showed that privacy nudges were powerful in altering users’ privacy attitudes, thereby facilitating users’ decision-making on information sharing.

Implications

This study attempted to address the contradicting recommendations for enhancing privacy-related behaviors and attitudes, the downplaying of privacy importance, and the argument that users do not care about privacy. This study indicated that users might exercise more control over personal information if they were given a choice. It has been argued that service providers require personal information to provide services (Fang et al., 2018), but the amount and extent of information collection

practices are not limited to what is needed to offer the services (Crossler & Bélanger, 2017)

Multiple researchers have studied the design of nudges (Acquisti et al., 2017; Tanaiutchawoot et al., 2019). Yee (2005) provided detailed guidelines for the design of the most effective nudges. Senju and Johnson (2009) found that nudges watching eyes are the most effective, while Masaki et al. (2020) found that nudges with general descriptions can be effective. The findings of this study suggest no significant difference between the different nudge designs, implying that having a nudge is adequate, regardless of the design.

The mobile application and the backend source codes will be publicly available for any researcher interested in building on top of this research. The application is built using the Flutter framework from Google, allowing the creation of both iOS and Android applications from a single code base.

Limitations

The study was conducted remotely by recruiting resources from MTurk and using an Android mobile application to simulate the service provider's information-sharing. A field study could have better evaluated the privacy nudges in situ on participants' own devices, which could have increased the ecological validity. The second limitation was the duration in which the participants kept the mobile application running on their phones. In an ideal situation, participants should have kept it for days or even weeks, during which more data could be collected under different circumstances. In this research, however, the majority of the participants kept the application running for only four hours, allowing for a limited number of nudges to be presented to the

participants without overloading them with notifications. Another limitation was the unavailability of an iOS application, which could have increased the number of participants and allowed the researcher to study how different device operating system owners act towards privacy.

Recommendations

Privacy nudges are an exciting topic with great potential for protecting personal information sharing (Acquisti et al., 2017). Users should be able to make efficient decisions regarding sharing personal information. Future work might include studying other factors that could influence the sharing of personal information. Cultural differences can be studied by including participants from different countries. Job functions could also be studied to better understand how different professionals act towards their data protection. Personality trait factors could also be included to understand how they could affect personal information sharing.

An iOS application could be made available to target a broader range of participants (not only from MTurk) to comply with Apple guidelines for publishing on the App Store. Privacy nudges could also be embodied in other mobile applications, such as social media or e-commerce applications, to better understand the users' preference for what information they feel comfortable sharing and what they do not. Future work might also include cooperation with one of the service providers to study the actual interest of their subscribers in having the ability to control their information sharing.

Since this study did not provide evidence for the effect of the privacy nudges on actual information sharing, future research could include the effect of nudges on

increasing the awareness of privacy practices employed by service providers. If a significant effect was found, then the effect of nudges could be significant on the intent to share personal information and then on the actual information sharing behavior.

Summary

This study focused on the intention to share personal information and the actual decision to share personal information and how it can be influenced through two distinct decision-making processes. A cognitive route occurs when the rational decision-making process is taken. The cognitive path was studied based on the trust level towards the service provider and how the trust level could affect personal information sharing and the awareness of the practices performed by the service providers to collect and process personal information. Trust level was found to have no significant influence on the decision-making process. However, awareness of data collection practices had a negative influence on personal information sharing. The heuristic decision-making route was studied using different privacy nudges. It was found that none of the nudge types had a statistically significant effect on sharing personal information. Age was studied as a moderating variable, but it did not significantly influence any of the variables in this study.

Appendix A
Questionnaire

Android Privacy Nudges Full Survey

Start of Block: Informed Consent



Q1

Welcome to the research study.

We are interested in understanding the factors affecting customers' decisions to share personal data with mobile operators. For this study, you will be presented with information relevant to sharing personal information with mobile operators. Then, you will be asked to answer some questions. Your responses will be kept confidential.

The study should take approximately 15 minutes to complete. After the survey, you should install the Privacy Nudges mobile application and follow the instructions. You will be compensated based on MTurk's terms and conditions. Your participation in this study is voluntary. You have the right to withdraw your participation at any point during the study. The principal investigator of this study can be contacted at aq123@mynsu.nova.edu.

By clicking the button below, you acknowledge that:

Your participation in the study is voluntary.

You are 18 years of age.

You are aware that you may choose to terminate your participation at any time for any reason.

-

I consent, begin the study (1)

I do not consent, I do not wish to participate (2)

End of Block: Informed Consent

Start of Block: Demographics



Q2 What is your year of birth?

Q3 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)

Q4 What is your MTurk ID? - It will be used to approve the HIT.

Q5 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)

Native Hawaiian or Pacific Islander (5)

Other (7)

Q6 What is your gender?

- Male (1)
 - Female (2)
 - Non-binary (3)
 - Prefer not to respond (4)
-

Q7 Information about income is very important for understanding. Please provide your best guess. 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)
-

Q8 On a daily basis, how long do you spend using your mobile device (on average) ?

- less than 1 hour (1)
 - 1 - 3 hours (2)
 - 4 - 6 hours (3)
 - 7 - 10 hours (4)
 - more than 10 hours (5)
-

Q9 What is the operating system on your smartphone ?

iOS (Apple) (1)

Android (Samsung, Google, Motorola..etc) (2)

Other (Windows, Blackberry...etc) (3)

Page Break

End of Block: Demographics

Start of Block: Mobile Company Trust



Q10 Which one is your current mobile service provider?

AT&T (1)

Verizon (2)

T-Mobile (3)

Sprint (4)

Virgin Mobile (5)

Boost (6)

Mint (7)

Google Fi (8)

Visible (9)

US Cellular (10)

Cricket (11)

MetroPCS (12)

Straight Talk (13)

Lyca (14)

Ting (15)

Other (16)

Page Break



Q11 I am familiar with \${Q10/ChoiceGroup/SelectedChoices}

- Strongly disagree (1)
 - Disagree (2)
 - Somewhat disagree (3)
 - Neither agree nor disagree (4)
 - Somewhat agree (5)
 - Agree (6)
 - Strongly agree (7)
-



Q12 If price were not a consideration, are you likely to purchase products or services from \${Q10/ChoiceGroup/SelectedChoices} in the future?

- Strongly disagree (1)
 - Disagree (2)
 - Somewhat disagree (3)
 - Neither agree nor disagree (4)
 - Somewhat agree (5)
 - Agree (6)
 - Strongly agree (7)
-

Page Break



Q13 I think the services from $\${Q10/ChoiceGroup/SelectedChoices}$ fit my practical needs.

- Strongly disagree (1)
 - Disagree (2)
 - Somewhat disagree (3)
 - Neither agree nor disagree (4)
 - Somewhat agree (5)
 - Agree (6)
 - Strongly agree (7)
-



Q14 How good or bad is the network quality of $\${Q10/ChoiceGroup/SelectedChoices}$?

- Extremely bad (1)
 - Moderately bad (2)
 - Slightly bad (3)
 - Neither good nor bad (4)
 - Slightly good (5)
 - Moderately good (6)
 - Extremely good (7)
-



Q15 In relation to other carriers in the marketplace, I think $\${Q10/ChoiceGroup/SelectedChoices}$ is trustworthy.

- Strongly disagree (1)
 - Disagree (2)
 - Somewhat disagree (3)
 - Neither agree nor disagree (4)
 - Somewhat agree (5)
 - Agree (6)
 - Strongly agree (7)
-



Q16 When you are thinking about purchasing a new service from [\\${Q10/ChoiceGroup/SelectedChoices}](#), you think privacy is important.

- Strongly disagree (1)
 - Disagree (2)
 - Somewhat disagree (3)
 - Neither agree nor disagree (4)
 - Somewhat agree (5)
 - Agree (6)
 - Strongly agree (7)
-



Q17 Overall, how good or bad was your experience using [\\${Q10/ChoiceGroup/SelectedChoices}](#) services?

- Extremely bad (1)
 - Moderately bad (2)
 - Slightly bad (3)
 - Neither good nor bad (4)
 - Slightly good (5)
 - Moderately good (6)
 - Extremely good (7)
-



Q18 Would you recommend [\\${Q10/ChoiceGroup/SelectedChoices}](#) to a friend or colleague?

- Strongly disagree (1)
- Disagree (2)
- Somewhat disagree (3)
- Neither agree nor disagree (4)
- Somewhat agree (5)
- Agree (6)
- Strongly agree (7)

Page Break



Q19 I believe in the future success of $\${Q10/ChoiceGroup/SelectedChoices}$

- Strongly disagree (1)
- Disagree (2)
- Somewhat disagree (3)
- Neither agree nor disagree (4)
- Somewhat agree (5)
- Agree (6)
- Strongly agree (7)



Q20 Do you think $\${Q10/ChoiceGroup/SelectedChoices}$ treats all of its customers fairly?

- Strongly disagree (1)
- Disagree (2)
- Somewhat disagree (3)
- Neither agree nor disagree (4)
- Somewhat agree (5)
- Agree (6)
- Strongly agree (7)



Q21 Services provided by $\{Q10/ChoiceGroup/SelectedChoices\}$, such as SMS/Texting or Voice calls, are secure.

- Strongly disagree (1)
- Disagree (2)
- Somewhat disagree (3)
- Neither agree nor disagree (4)
- Somewhat agree (5)
- Agree (6)
- Strongly agree (7)



Q22 Communications through mobile phones are safe?

- Strongly disagree (1)
- Disagree (2)
- Somewhat disagree (3)
- Neither agree nor disagree (4)
- Somewhat agree (5)
- Agree (6)
- Strongly agree (7)

Page Break

End of Block: Mobile Company Trust

Start of Block: Amount and type of requested data



Q23 I am aware that my physical location is being tracked by
\${Q10/ChoiceGroup/SelectedChoices}

- Strongly disagree (1)
 - Disagree (2)
 - Somewhat disagree (3)
 - Neither agree nor disagree (4)
 - Somewhat agree (5)
 - Agree (6)
 - Strongly agree (7)
-



Q24 I am aware of how \${Q10/ChoiceGroup/SelectedChoices} can access my information.

- Strongly disagree (1)
 - Disagree (2)
 - Somewhat disagree (3)
 - Neither agree nor disagree (4)
 - Somewhat agree (5)
 - Agree (6)
 - Strongly agree (7)
-



Q25 I know how to protect my personal data on my phone and when I use a public network.

- Strongly disagree (1)
 - Disagree (2)
 - Somewhat disagree (3)
 - Neither agree nor disagree (4)
 - Somewhat agree (5)
 - Agree (6)
 - Strongly agree (7)
-



Q26 Users have control over how their personal information is collected and shared by mobile companies.

- Strongly disagree (1)
 - Disagree (2)
 - Somewhat disagree (3)
 - Neither agree nor disagree (4)
 - Somewhat agree (5)
 - Agree (6)
 - Strongly agree (7)
-



Q27 Mobile companies handle the personal information they collect in a proper and confidential way

- Strongly disagree (1)
 - Disagree (2)
 - Somewhat disagree (3)
 - Neither agree nor disagree (4)
 - Somewhat agree (5)
 - Agree (6)
 - Strongly agree (7)
-



Q28 Existing laws and regulations enforce a reasonable level of protection for consumer privacy today

- Strongly disagree (1)
 - Disagree (2)
 - Somewhat disagree (3)
 - Neither agree nor disagree (4)
 - Somewhat agree (5)
 - Agree (6)
 - Strongly agree (7)
-



Q29 I do not need a security tool such as a VPN service when sharing sensitive information over public networks.

Strongly disagree (1)

Disagree (2)

Somewhat disagree (3)

Neither agree nor disagree (4)

Somewhat agree (5)

Agree (6)

Strongly agree (7)



Q30 As a result of using my mobile phone, information about me that I consider private is more available to others that I dont want

Strongly disagree (1)

Disagree (2)

Somewhat disagree (3)

Neither agree nor disagree (4)

Somewhat agree (5)

Agree (6)

Strongly agree (7)



Q31 As a result of using my mobile phone, I feel there is information about me that if used, it will invade my privacy.

- Strongly disagree (1)
 - Disagree (2)
 - Somewhat disagree (3)
 - Neither agree nor disagree (4)
 - Somewhat agree (5)
 - Agree (6)
 - Strongly agree (7)
-



Q32 As a result of using my mobile phone, I am concerned that my personal information could be used by $\${Q10/ChoiceGroup/SelectedChoices}$ without my acceptance

- Strongly disagree (1)
 - Disagree (2)
 - Somewhat disagree (3)
 - Neither agree nor disagree (4)
 - Somewhat agree (5)
 - Agree (6)
 - Strongly agree (7)
-



Q33 As a result of using my mobile phone, I feel that $\${Q10/ChoiceGroup/SelectedChoices}$ knows sensitive information about me that I am concerned about

- Strongly agree (1)
 - Agree (2)
 - Somewhat agree (3)
 - Neither agree nor disagree (4)
 - Somewhat disagree (5)
 - Disagree (6)
 - Strongly disagree (7)
-

Page Break

End of Block: Amount and type of requested data

Start of Block: Sharing personal information with service provider



Q34 It is safe to trade my phone with $\${Q10/ChoiceGroup/SelectedChoices}$.

- Strongly disagree (1)
 - Disagree (2)
 - Somewhat disagree (3)
 - Neither agree nor disagree (4)
 - Somewhat agree (5)
 - Agree (6)
 - Strongly agree (7)
-



Q35 I would share your phone book (contact list) with $\${Q10/ChoiceGroup/SelectedChoices}$.

- Strongly agree (1)
 - Agree (2)
 - Somewhat agree (3)
 - Neither agree nor disagree (4)
 - Somewhat disagree (5)
 - Disagree (6)
 - Strongly disagree (7)
-



Q36 I agree with sharing my physical location history with [\\${Q10/ChoiceGroup/SelectedChoices}](#).

- Strongly agree (1)
 - Agree (2)
 - Somewhat agree (3)
 - Neither agree nor disagree (4)
 - Somewhat disagree (5)
 - Disagree (7)
 - Strongly disagree (8)
-



Q37 I share sensitive information through my mobile phone

- Strongly disagree (1)
 - Disagree (2)
 - Somewhat disagree (3)
 - Neither agree nor disagree (4)
 - Somewhat agree (5)
 - Agree (6)
 - Strongly agree (7)
-



Q38 I limit sensitive data through my phone, because I am concerned that [\\${Q10/ChoiceGroup/SelectedChoices}](#) could use my information without informing me or taking my authorization.

- Strongly disagree (1)
 - Disagree (2)
 - Somewhat disagree (3)
 - Neither agree nor disagree (4)
 - Somewhat agree (5)
 - Agree (6)
 - Strongly agree (7)
-



Q39 How comfortable are you with the amount of data other businesses know about you, as a result of using `$$Q10/ChoiceGroup/SelectedChoices`?

- Extremely comfortable (1)
 - Moderately comfortable (2)
 - Slightly comfortable (3)
 - Neither comfortable nor uncomfortable (4)
 - Slightly uncomfortable (5)
 - Moderately uncomfortable (6)
 - Extremely uncomfortable (7)
-



Q40 When I was younger, I used to share more information on my phone.

- Strongly disagree (1)
- Disagree (2)
- Somewhat disagree (3)
- Neither agree nor disagree (4)
- Somewhat agree (5)
- Agree (6)
- Strongly agree (7)

End of Block: Sharing personal information with service provider

Appendix B

Institutional Review Board



MEMORANDUM

To: Ammar Qaffaf
College of Engineering and Computing

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

Date: January 7, 2021

Subject: IRB Exempt Initial Approval Memo

TITLE: Factors Affecting Customers' Decision to Share Personal Data with Mobile Operators– NSU IRB Protocol Number 2021-8

Dear Principal Investigator,

Your submission has been reviewed and Exempted by your IRB College Representative or their Alternate on **January 5, 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

Page 1 of 2

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

- Ab Hamid, M. R., Sami, W., & Mohmad Sidek, M. H. (2017). Discriminant Validity Assessment: Use of Fornell & Larcker criterion versus HTMT Criterion. *Journal of Physics: Conference Series*, 890(1), 0–5. <https://doi.org/10.1088/1742-6596/890/1/012163>
- Abdelrazek, L., & Azer, M. A. (2019). User privacy in legacy mobile network protocols. *Proceedings of the 2018 3rd International Conference on System Reliability and Safety, ICSRS 2018*, 109–114. <https://doi.org/10.1109/ICSRS.2018.8688870>
- Acquisti, A. (2009). Nudging privacy: The behavioral economics of personal information. *IEEE Security and Privacy*, 7(6), 82–85. <https://doi.org/10.1109/MSP.2009.163>
- Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y., & Wilson, S. (2017). Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys*, 50(3), 1–41. <https://doi.org/10.1145/3054926>
- Acquisti, A., Adjerid, I., & Brandimarte, L. (2013). Gone in 15 seconds: The limits of privacy transparency and control. *IEEE Security & Privacy*, 11(4), 72–74. <https://doi.org/10.1109/MSP.2013.86>
- Acquisti, A., & Grossklags, J. (2007). *What can behavioral economics teach us about privacy?* (1st ed.). Auerbach Publications.
- Acquisti, A., & Grossklags, J. (2012). An online survey experiment on ambiguity and privacy. *Communications and Strategies*, 1(88), 19–39.
- Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature*, 54(2), 442–492. <https://doi.org/10.1257/jel.54.2.442>
- Agarwal, V., Mittal, S., Mukherjea, S., & Dalal, P. (2012). Exploiting rich telecom data for increased monetization of telecom application stores. *2012 IEEE 13th International Conference on Mobile Data Management*, 63–68. <https://doi.org/10.1109/MDM.2012.28>
- Ahmad, A. K., Jafar, A., & Aljoumaa, K. (2019). Customer churn prediction in telecom using machine learning in big data platform. *Journal of Big Data*, 6(1). <https://doi.org/10.1186/s40537-019-0191-6>
- Aïmeur, E. (2018). Personalisation and privacy issues in the age of exposure. *UMAP 2018 - Proceedings of the 26th Conference on User Modeling, Adaptation and Personalization*, 375–376. <https://doi.org/10.1145/3209219.3209271>

- Aïmeur, E., Lawani, O., & Dalkir, K. (2016). When changing the look of privacy policies affects user trust: An experimental study. *Computers in Human Behavior*, 58, 368–379. <https://doi.org/10.1016/j.chb.2015.11.014>
- Alemaný, J., del Val, E., Alberola, J., & García-Fornes, A. (2019). Enhancing the privacy risk awareness of teenagers in online social networks through soft-paternalism mechanisms. *International Journal of Human Computer Studies*, 129(March), 27–40. <https://doi.org/10.1016/j.ijhcs.2019.03.008>
- Almuhimedi, H. (2017). Helping users manage their privacy through nudges. In *Doctoral dissertation, Carnegie Mellon University*. <https://doi.org/10.1184/r1/6719579.v1>
- Almuhimedi, H., Felt, A. P., Reeder, R. W., & Consolvo, S. (2014). Your reputation precedes you: History, reputation, and the Chrome malware warning. *SOUPS '14: Proceedings of the Tenth Symposium On Usable Privacy and Security*, 113–128. <https://www.usenix.org/conference/soups2014/proceedings/presentation/almuhimedi>
- Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly: Management Information Systems*, 30(1), 13–28. <https://doi.org/10.2307/25148715>
- Bal, P. M., De Lange, A. H., Ybema, J. F., Jansen, P. G. W., & Van Der Velde, M. E. G. (2011). Age and trust as moderators in the relation between procedural justice and turnover: A large-scale longitudinal study. *Applied Psychology*, 60(1), 66–86. <https://doi.org/10.1111/j.1464-0597.2010.00427.x>
- Balapour, A., Nikkhah, H. R., & Sabherwal, R. (2020). Mobile application security: Role of perceived privacy as the predictor of security perceptions. *International Journal of Information Management*, 52(January), 102063. <https://doi.org/10.1016/j.ijinfomgt.2019.102063>
- Balebako, R., Leon, P. G., Almuhimedi, H., Kelley, P. G., Mugan, J., Acquisti, A., Cranor, L. F., & Sadeh, N. (2011). Nudging users towards privacy on mobile devices. *CEUR Workshop Proceedings*, 722, 23–26.
- Bansal, G., Zahedi, F. M., & Gefen, D. (2008). The moderating influence of privacy concern on the efficacy of privacy assurance mechanisms for building trust: A multiple-context investigation | L'effet modérateur du souci de confidentialité sur l'efficacité des mécanismes de respect de la vie privée à. *Proceedings of the ICIS 2008 Twenty Ninth International Conference on Information Systems*, 7.
- Barev, T. J., Schwede, M., & Janson, A. (2021). The dark side of privacy nudging - An experimental study in the context of a digital work environment. *Proceedings of the Annual Hawaii International Conference on System Sciences, 2020-Janua*(Figure 3), 4114–4123. <https://doi.org/10.24251/hicss.2021.500>

- Barth, S., de Jong, M. D. T., Junger, M., Hartel, P. H., & Roppelt, J. C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and Informatics*, *41*(November 2017), 55–69. <https://doi.org/10.1016/j.tele.2019.03.003>
- Bashir, M., Hoff, K. A., Hayes, C. M., & Kesan, J. P. (2014). Knowledge-based individualized privacy plans (KIPPs): A potential tool to improve the effectiveness of privacy notices. *Proceedings of the Workshop on the Future of Privacy Notice and Choice*, 27.
- Belanger, F., & Crossler, R. E. (2019). Dealing with digital traces: Understanding protective behaviors on mobile devices. *Journal of Strategic Information Systems*, *28*(1), 34–49. <https://doi.org/10.1016/j.jsis.2018.11.002>
- Benndorf, V., & Normann, H. (2018). The willingness to sell personal data. *The Scandinavian Journal of Economics*, *120*(4), 1260–1278. <https://doi.org/10.1111/sjoe.12247>
- Bergram, K., Gjerlufsen, T., Maingot, P., Bezencon, V., & Holzer, A. (2020). Digital nudges for privacy awareness: From consent to informed consent? *Proceedings of the 28th European Conference on Information Systems (ECIS)*, 1–16. https://aisel.aisnet.org/ecis2020_rp/64
- Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013). Digital business strategy: Toward a next generation of insights. *MIS Quarterly: Management Information Systems*, *37*(2), 471–482. <https://doi.org/10.25300/MISQ/2013/37:2.3>
- Bodi, M., le Rouzic, J.-P., Hiribarren, V., Jain, M., & Maurologoitia, J. (2010). Personalization enablers by Telecom operators. *Proceedings of the 2010 IEEE Globecom Workshops, 2022–2027*. <https://doi.org/10.1109/GLOCOMW.2010.5700299>
- Brandtzaeg, P. B., Pultier, A., & Moen, G. M. (2019). Losing control to data-hungry apps: A mixed-methods approach to mobile app privacy. *Social Science Computer Review*, *37*(4), 466–488. <https://doi.org/10.1177/0894439318777706>
- Buchanan, E. M., & Scofield, J. E. (2018). Methods to detect low quality data and its implication for psychological research. *Behavior Research Methods*, *50*(6), 2586–2596. <https://doi.org/10.3758/s13428-018-1035-6>
- Buchwald, A., Letner, A., Urbach, N., & Von Entreeß-Fürsteneck, M. (2017). Towards explaining the willingness to disclose personal self-tracking data to service providers. *Proceedings of the 25th European Conference on Information Systems, ECIS 2017, 2017*, 3071–3081.

- Cadzow, S. W. (2012). Privacy: The forgotten challenge in sensor and distributed systems. *Proceedings of the IET Conference on Wireless Sensor Systems (WSS 2012)*, 2012(601 CP), 4B2-4B2. <https://doi.org/10.1049/cp.2012.0594>
- California State Legislature. (2018). AB-375 Privacy: Personal information: businesses. (CCPA). *Legislative Counsel's Digest*, 55(375), 24. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375
- Carrascal, J. P., Riederer, C., Erramilli, V., Cherubini, M., & De Oliveira, R. (2013). Your browsing behavior for a big mac: Economics of personal information online. *WWW 2013 - Proceedings of the 22nd International Conference on World Wide Web*, 189–199.
- Casadesus-Masanell, R., & Hervas-Drane, A. (2020). Strategies for managing the privacy landscape. *Long Range Planning*, 53(4), 101949. <https://doi.org/10.1016/j.lrp.2019.101949>
- Case, C. J., & King, D. L. (2021). Fair information practices: An empirical review of the Fortune 500. *ASBBS Proceedings*, 28, 60–70.
- Chakraborty, S., & Tripp, O. (2016). Eavesdropping and obfuscation techniques for smartphones. *Proceedings of the International Conference on Mobile Software Engineering and Systems*, 291–292. <https://doi.org/10.1145/2897073.2897715>
- Chellappa, R. K. (2002). Consumers' trust in electronic commerce transactions: The role of perceived privacy and perceived security. In *Thesis*. Emory University Atlanta.
- Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management*, 6(2–3), 181–202. <https://doi.org/10.1007/s10799-005-5879-y>
- Chin, W. W. (1998). The partial least squares approach to structural equation modelling. In Marcoulides G. A. (Ed.). *Modern Methods for Business Research*, 295(2), 295–336.
- Choi, J. P., Jeon, D. S., & Kim, B. C. (2019). Privacy and personal data collection with information externalities. *Journal of Public Economics*, 173, 113–124. <https://doi.org/10.1016/j.jpubeco.2019.02.001>
- Christl, W. (2017). How companies use personal data against people. Automated disadvantage, personalized persuasion, and the societal ramifications of the commercial use of personal information. *Cracked Lab – Institute for Critical Digital Culture*, October. <http://crackedlabs.org/en/data-against-people>

- Cohen, J. (1992). A power primer. *Psychological Bulletin*, 112(1), 155–159.
<https://doi.org/10.1037/0033-2909.112.1.155>
- Comcast Corporation. (2018). Comcast 2018 Annual Report. *Securities and Exchange Commission*.
- Cranor, L. F., Hoke, C., Leon, P., & Au, A. (2018). Are they worth reading? An in-depth analysis of online advertising companies privacy policies. *SSRN Electronic Journal, Tprc*. <https://doi.org/10.2139/ssrn.2418590>
- Creswell, J. W. (2014). *The selection of a research approach* (4th ed.). SAGE Publications.
- Crossler, R. E., & Bélanger, F. (2017). The mobile privacy-security knowledge gap model: Understanding behaviors. *Proceedings of the 50th Hawaii International Conference on System Sciences (2017)*, 4071–4080.
<https://doi.org/10.24251/hicss.2017.491>
- Culnan, M. J., & Williams, C. C. (2009). How ethics can enhance organizational privacy: Lessons from the ChoicePoint and TJX data breaches. *MIS Quarterly: Management Information Systems*, 33(4), 673–687.
<https://doi.org/10.2307/20650322>
- Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1), 61–80.
<https://doi.org/10.1287/isre.1060.0080>
- Dogruel, L., Joeckel, S., & Vitak, J. (2017). The valuation of privacy premium features for smartphone apps: The influence of defaults and expert recommendations. *Computers in Human Behavior*, 77, 230–239.
<https://doi.org/10.1016/j.chb.2017.08.035>
- Dowding, M. (2014). The internet tree: The state of telecom policy in Canada 3.0. *Canadian Journal of Communication*, 39(3), 3.
<https://doi.org/10.22230/cjc.2014v39n3a2904>
- Dowthwaite, L., Creswick, H., Portillo, V., Zhao, J., Patel, M., Vallejos, E. P., Koene, A., & Jirotko, M. (2020). It's your private information. it's your life.: Young people's views of personal data use by online technologies. *Proceedings of the Interaction Design and Children Conference, IDC 2020*, 121–134.
<https://doi.org/10.1145/3392063.3394410>
- Elvy, S. A. (2017). Paying for privacy and the personal data economy. *Columbia Law Review*, 117(6), 1369–1460.

- Fahey, R. A., & Hino, A. (2020). COVID-19, digital privacy, and the social limits on data-focused public health responses. *International Journal of Information Management*, 55(July), 102181. <https://doi.org/10.1016/j.ijinfomgt.2020.102181>
- Falivene, L. I. (2021). *Understanding the privacy awareness gap*. Carnegie Mellon University.
- Fang, D., Qian, Y., & Hu, R. Q. (2018). Security for 5G Mobile Wireless Networks. *IEEE Access*, 6, 4850–4874. <https://doi.org/10.1109/ACCESS.2017.2779146>
- Felt, A. P., Reeder, R. W., Almuhimedi, H., & Consolvo, S. (2014). Experimenting at scale with google chrome's SSL warning. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2667–2670. <https://doi.org/10.1145/2556288.2557292>
- Garg, V., Benton, K., & Camp, L. J. (2014). The privacy paradox: A Facebook case study. *Proceedings of the TRPC 42: The 42nd Research Conference on Communication, Information and Internet Policy*. <https://doi.org/10.2139/ssrn.2411672>
- Geller, T. (2016). In privacy law, it's the U.S. vs. the world. *Communications of the ACM*, 59(2), 21–23. <https://doi.org/10.1145/2852233>
- Golle, P. (2006). Revisiting the uniqueness of simple demographics in the US population. *Proceedings of the ACM Conference on Computer and Communications Security*, 77–80. <https://doi.org/10.1145/1179601.1179615>
- Grabowski, P., & Samfelt, J. (2016). User awareness of privacy regarding user data in mobile health applications and wearables: Do you know what you are sharing? In *Master thesis, Lund University*.
- Gu, J., Xu, Y. (Calvin), Xu, H., Zhang, C., & Ling, H. (2017). Privacy concerns for mobile app download: An elaboration likelihood model perspective. *Decision Support Systems*, 94, 19–28. <https://doi.org/10.1016/j.dss.2016.10.002>
- Hermet, G., & Combet, J. (2011). Mobile internet monetization: A methodology to monitor in real time the cellular subscriber transactional itinerary, from mobile advertising exposure to actual purchase. *Proceedings of the 2011 10th International Conference on Mobile Business*, 307–312. <https://doi.org/10.1109/ICMB.2011.20>
- Heurix, J., Zimmermann, P., Neubauer, T., & Fenz, S. (2015). A taxonomy for privacy enhancing technologies. *Computers and Security*, 53, 1–17. <https://doi.org/10.1016/j.cose.2015.05.002>

- Ho, S. Y., & Bodoff, D. (2014). The effects of web personalization on user attitude and behavior: An integration of the Elaboration Likelihood Model and Consumer Search Theory. *MIS Quarterly*, 38(2), 497–520. <https://doi.org/10.25300/MISQ/2014/38.2.08>
- Hoa, C.-T. B., & Choub, Y.-H. D. (2014). The effects of trust for online auction: Elaboration Likelihood Model. *Online Book of Proceedings IRC 2014*, 25–26.
- Höhne, J. K., & Lenzner, T. (2018). New insights on the cognitive processing of agree/disagree and item-specific questions. *Journal of Survey Statistics and Methodology*, 6(3), 401–417. <https://doi.org/10.1093/JSSAM/SMX028>
- Hong, C.-G., & Dietze, C. (2019). Enabling digital excellence through business process management and process frameworks. In P. Krüssel (Ed.), *Future Telco* (pp. 341–348). Springer International Publishing. https://doi.org/10.1007/978-3-319-77724-5_30
- Hossain, M. A., Akter, S., & Yanamandram, V. (2020). Revisiting customer analytics capability for data-driven retailing. *Journal of Retailing and Consumer Services*, 56(June), 102187. <https://doi.org/10.1016/j.jretconser.2020.102187>
- Hsu, C.-L., & Wu, C.-C. (2012). Understanding users' continuance of Facebook. *International Journal of Virtual Communities and Social Networking*, 3(2), 1–16. <https://doi.org/10.4018/jvcsn.2011040101>
- Huang, H. Y., & Bashir, M. (2016). The onion router: Understanding a privacy enhancing technology community. *Proceedings of the Association for Information Science and Technology*, 53(1), 1–10. <https://doi.org/10.1002/pr2.2016.14505301034>
- Huberman, B. A., Adar, E., & Fine, L. R. (2005). Valuating privacy. *IEEE Security and Privacy Magazine*, 3(5), 22–25. <https://doi.org/10.1109/MSP.2005.137>
- Hubert, M., Blut, M., Brock, C., Backhaus, C., & Eberhardt, T. (2017). Acceptance of smartphone-based mobile shopping: Mobile benefits, customer characteristics, perceived risks, and the impact of application context. *Psychology & Marketing*, 34(2), 175–194. <https://doi.org/10.1002/mar.20982>
- Jackson, C. B., & Wang, Y. (2018). Addressing the privacy paradox through personalized privacy notifications. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 2(2), 1–25. <https://doi.org/10.1145/3214271>
- Johnson, M. L. (2012). Toward usable access control for end-users: A case study of Facebook privacy settings. *ProQuest Dissertations and Theses*, 152. <https://search.proquest.com/docview/1112476777?accountid=14169>

- Joshi, S., Dalal, R., Egbert, R. C., & Chaudhary, A. (2016). Telecom-OTT partnership: Generating new revenue sharing models. *Telecom Business Review*, 9(1), 21–31. <http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=120058434&site=ehost-live>
- Kittur, A., Chi, E. H., & Suh, B. (2008). Crowdsourcing user studies with Mechanical Turk. *Proceeding of the Twenty-Sixth Annual CHI Conference on Human Factors in Computing Systems - CHI '08*, 453. <https://doi.org/10.1145/1357054.1357127>
- Kobsa, A., Cho, H., & Knijnenburg, B. P. (2016). The effect of personalization provider characteristics on privacy attitudes and behaviors: An Elaboration Likelihood Model approach. *Journal of the Association for Information Science and Technology*, 67(11), 2587–2606. <https://doi.org/10.1002/asi.23629>
- Kock, N., & Hadaya, P. (2018). Minimum sample size estimation in PLS-SEM: The inverse square root and gamma-exponential methods. *Information Systems Journal*, 28(1), 227–261. <https://doi.org/10.1111/isj.12131>
- Krasnova, H., & Veltri, N. F. (2010). Privacy calculus on social networking sites: Explorative evidence from Germany and USA. *Proceedings of the 2010 43rd Hawaii International Conference on System Sciences*, 1–10. <https://doi.org/10.1109/HICSS.2010.307>
- Kugler, L. (2018). The war over the value of personal data. *Communications of the ACM*, 61(2), 17–19. <https://doi.org/10.1145/3171580>
- Lalmas, M. (2019). Engagement, metrics and personalisation. *Proceedings of the 27th ACM Conference on User Modeling, Adaptation and Personalization*, 2–2. <https://doi.org/10.1145/3320435.3323709>
- Lane, N. D. (2012). Community-aware smartphone sensing systems. *IEEE Internet Computing*, 16(3), 60–64. <https://doi.org/10.1109/MIC.2012.48>
- Larose, R., & Rifon, N. (2006). Your privacy is assured-of being disturbed: Websites with and without privacy seals. *New Media and Society*, 8(6), 1009–1029. <https://doi.org/10.1177/1461444806069652>
- Leon, P. G., Ur, B., Wang, Y., Sleeper, M., Balebako, R., Shay, R., Bauer, L., Christodorescu, M., & Cranor, L. F. (2013). What matters to users? Factors that affect users' willingness to share information with online advertisers. *SOUPS 2013 - Proceedings of the 9th Symposium on Usable Privacy and Security, May 2014*. <https://doi.org/10.1145/2501604.2501611>
- Leppäniemi, M., Karjaluoto, H., & Saarijärvi, H. (2017). Customer perceived value, satisfaction, and loyalty: the role of willingness to share information. *The International Review of Retail, Distribution and Consumer Research*, 27(2), 164–188. <https://doi.org/10.1080/09593969.2016.1251482>

- Levin, H., Egger, D., Johnson, M., & Barbaro, K. de. (2013). Parent willingness to collect and share children's mobile-sensing data. *Journal of Chemical Information and Modeling*, 53(9), 1689–1699. <https://doi.org/10.31234/osf.io/u39xg>
- Li, & Unger, T. (2012). Willing to pay for quality personalization Trade-off between quality and privacy. *European Journal of Information Systems*, 21(6), 621–642. <https://doi.org/10.1057/ejis.2012.13>
- Li, X. B., & Raghunathan, S. (2014). Pricing and disseminating customer data with privacy awareness. *Decision Support Systems*, 59(1), 63–73. <https://doi.org/10.1016/j.dss.2013.10.006>
- Limba, T., & Šidlauskas, A. (2018). Secure personal data administration in the social networks: the case of voluntary sharing of personal data on the Facebook. *Entrepreneurship and Sustainability Issues*, 5(3), 528–541. [https://doi.org/10.9770/jesi.2018.5.3\(9\)](https://doi.org/10.9770/jesi.2018.5.3(9))
- Liu, Z., Shan, J., & Pigneur, Y. (2016). The role of personalized services and control: An empirical evaluation of privacy calculus and technology acceptance model in the mobile context. *Journal of Information Privacy and Security*, 12(3), 123–144. <https://doi.org/10.1080/15536548.2016.1206757>
- Liyanage, M., Salo, J., Braeken, A., Kumar, T., Seneviratne, S., & Ylianttila, M. (2018). 5G privacy: Scenarios and solutions. *Proceedings of 2018 IEEE 5G World Forum (5GWF)*, 197–203. <https://doi.org/10.1109/5GWF.2018.8516981>
- Lowry, P. B., Moody, G., Vance, A., Jensen, M., Jenkins, J., & Wells, T. (2012). Using an elaboration likelihood approach to better understand the persuasiveness of website privacy assurance cues for online consumers. *Journal of the American Society for Information Science and Technology*, 63(4), 755–776. <https://doi.org/10.1002/asi.21705>
- Malgieri, G., & Custers, B. (2018). Pricing privacy – the right to know the value of your personal data. *Computer Law & Security Review*, 34(2), 289–303. <https://doi.org/10.1016/j.clsr.2017.08.006>
- 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>
- Mamonov, S., & Benbunan-Fich, R. (2018). The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior*, 83, 32–44. <https://doi.org/10.1016/j.chb.2018.01.028>
- Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, 81(1), 36–58. <https://doi.org/10.1509/jm.15.0497>

- Masaki, H., Shibata, K., Hoshino, S., Ishihama, T., Saito, N., & Yatani, K. (2020). Exploring nudge designs to help adolescent SNS users avoid privacy and safety threats. *Conference on Human Factors in Computing Systems - Proceedings*, 1–11. <https://doi.org/10.1145/3313831.3376666>
- 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>
- Miaoui, Y., Boudriga, N., & Abaoub, E. (2015). Economics of privacy: A model for protecting against cyber data disclosure attacks. *Procedia Computer Science*, 72, 569–579. <https://doi.org/10.1016/j.procs.2015.12.165>
- Milberg, S. J., Burke, S. J., Smith, H. J., & Kallman, E. A. (1995). Values, personal information privacy, and regulatory approaches. *Communications of the ACM*, 38(12), 65–74. <https://doi.org/10.1145/219663.219683>
- Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing*, 18(3), 15–29. <https://doi.org/10.1002/dir.20009>
- Miltgen, C. L. (2009). Online consumer privacy concerns and willingness to provide personal data on the internet. *International Journal of Networking and Virtual Organisations*, 6(6), 574–603. <https://doi.org/10.1504/IJNVO.2009.027790>
- Minonne, C., Wyss, R., Schwer, K., Wirz, D., & Hitz, C. (2018). Digital maturity variables and their impact on the enterprise architecture layers. *Problems and Perspectives in Management*, 16(4), 141–154. [https://doi.org/10.21511/ppm.16\(4\).2018.13](https://doi.org/10.21511/ppm.16(4).2018.13)
- Mohr, B., Dolgoplova, I., & Roosen, J. (2019). The influence of sex and self-control on the efficacy of nudges in lowering the energy content of food during a fast food order. *Appetite*, 141(June), 104314. <https://doi.org/10.1016/j.appet.2019.06.006>
- Mousavi, R., Chen, R., Kim, D. J., & Chen, K. (2020). Effectiveness of privacy assurance mechanisms in users' privacy protection on social networking sites from the perspective of protection motivation theory. *Decision Support Systems*, 135(September 2019), 113323. <https://doi.org/10.1016/j.dss.2020.113323>
- Mraznica, E. (2017). GDPR: A new challenge for personal data protection. *Bankarstvo*, 46(4), 166–177. <https://doi.org/10.5937/bankarstvo1704166m>
- Nissenbaum, H. (1997). Toward an approach to privacy in public: Challenges of information technology. *Ethics & Behavior*, 7(3), 207–219. https://doi.org/10.1207/s15327019eb0703_3
- Ohm, P. (2010). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Review*, 57(6), 1701–1777.

- Palmerino, J. (2018). Improving Android permissions models for increased user awareness and security. *Proceedings of the 5th International Conference on Mobile Software Engineering and Systems*, 41–42. <https://doi.org/10.1145/3197231.3198446>
- Paramarta, V., Jihad, M., Dharma, A., Hapsari, I. C., Sandhyaduhita, P. I., & Hidayanto, A. N. (2019). Impact of user awareness, trust, and privacy concerns on sharing personal information on social media: Facebook, twitter, and instagram. *2018 International Conference on Advanced Computer Science and Information Systems, ICACISIS 2018*, 271–276. <https://doi.org/10.1109/ICACISIS.2018.8618220>
- Pentina, I., Zhang, L., Bata, H., & Chen, Y. (2016). Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison. *Computers in Human Behavior*, *65*, 409–419. <https://doi.org/10.1016/j.chb.2016.09.005>
- Peruma, A., Palmerino, J., & Krutz, D. E. (2018). Investigating user perception and comprehension of Android permission models. *Proceedings of the International Conference on Software Engineering*, 56–66. <https://doi.org/10.1145/3197231.3197246>
- Pitkänen, O., & Tuunainen, V. K. (2012). Disclosing personal data socially — An empirical study on Facebook users' privacy awareness. *Journal of Information Privacy and Security*, *8*(1), 3–29. <https://doi.org/10.1080/15536548.2012.11082759>
- Pu, Y., & Grossklags, J. (2019). Valuating friends' privacy: Does anonymity of sharing personal data matter? *Proceedings of the 13th Symposium on Usable Privacy and Security, SOUPS 2017, SOUPS*, 339–355. <https://www.usenix.org/system/files/conference/soups2017/soups2017-pu.pdf>
- Quay-De La Vallee, H., Selby, P., & Krishnamurthi, S. (2016). On a (Per)Mission: Building privacy into the app marketplace. *SPSM 2016 - Proceedings of the 6th Workshop on Security and Privacy in Smartphones and Mobile Devices, Co-Located with CCS 2016*, 63–72. <https://doi.org/10.1145/2994459.2994466>
- Rao, S. P., Kotte, B. T., & Holtmanns, S. (2016). Privacy in LTE networks. *Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications*, 176–183. <https://doi.org/10.4108/eai.18-6-2016.2264393>
- Räsänen, P., & Koironen, I. (2016). Changing patterns of ICT use in Finland - The senior citizens' perspective. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Vol. 9754). https://doi.org/10.1007/978-3-319-39943-0_22

- Rasi, P., & Kilpeläinen, A. (2016). Older people's use and learning of new media: A case study on remote rural villages in Finnish Lapland. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Vol. 9755). https://doi.org/10.1007/978-3-319-39949-2_23
- Renaud, K., & Zimmermann, V. (2018). Ethical guidelines for nudging in information security & privacy. *International Journal of Human Computer Studies*, 120(January), 22–35. <https://doi.org/10.1016/j.ijhcs.2018.05.011>
- Reychav, I., & Weisberg, J. (2010). Bridging intention and behavior of knowledge sharing. *Journal of Knowledge Management*, 14(2), 285–300. <https://doi.org/10.1108/13673271011032418>
- Ringle, C. M., Wende, S., & Becker, J.-M. (2015). *SmartPLS 3*. Bönningstedt: SmartPLS. <https://www.smartpls.com>
- Robinson, C. (2017). Disclosure of personal data in ecommerce: A cross-national comparison of Estonia and the United States. *Telematics and Informatics*, 34(2), 569–582. <https://doi.org/10.1016/j.tele.2016.09.006>
- Robinson, S. C. (2017). Self-Disclosure and managing privacy: Implications for interpersonal and online communication for consumers and marketers. *Journal of Internet Commerce*, 16(4), 385–404. <https://doi.org/10.1080/15332861.2017.1402637>
- Robinson, S. C. (2018). Factors predicting attitude toward disclosing personal data online. *Journal of Organizational Computing and Electronic Commerce*, 28(3), 214–233. <https://doi.org/10.1080/10919392.2018.1482601>
- Rodríguez-Priego, N., van Bavel, R., & Monteleone, S. (2016). The disconnection between privacy notices and information disclosure: an online experiment. *Economia Politica*, 33(3), 433–461. <https://doi.org/10.1007/s40888-016-0040-4>
- Rueben, M., Bernieri, F. J., Grimm, C. M., & Smart, W. D. (2017). Framing effects on privacy concerns about a home telepresence robot. *Proceedings of the 2017 ACM/IEEE International Conference on Human-Robot Interaction, Part F1271*, 435–444. <https://doi.org/10.1145/2909824.3020218>
- Saborido, R., Khomh, F., Antoniol, G., & Gueheneuc, Y.-G. (2017). Comprehension of ads-supported and paid Android applications: Are they different? *Proceeding of 2017 IEEE/ACM 25th International Conference on Program Comprehension (ICPC)*, 143–153. <https://doi.org/10.1109/ICPC.2017.25>
- Sætra, H. S. (2019). When nudge comes to shove: Liberty and nudging in the era of big data. *Technology in Society*, 59(April), 101130. <https://doi.org/10.1016/j.techsoc.2019.04.006>

- Schneider, M. J., Jagpal, S., Gupta, S., Li, S., & Yu, Y. (2017). Protecting customer privacy when marketing with second-party data. *International Journal of Research in Marketing*, 34(3), 593–603. <https://doi.org/10.1016/j.ijresmar.2017.02.003>
- Senju, A., & Johnson, M. H. (2009). The eye contact effect: mechanisms and development. *Trends in Cognitive Sciences*, 13(3), 127–134. <https://doi.org/10.1016/j.tics.2008.11.009>
- Shih, F., Liccardi, I., & Weitzner, D. (2015). Privacy tipping points in smartphones privacy preferences. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, 2015-April*, 807–816. <https://doi.org/10.1145/2702123.2702404>
- Shin, J., Cho, D., & Sim, J. (2017). Concerns make your decision better: Privacy perception, increased awareness, and the decision of mobile app installation. *Proceedings of the 21st Pacific Asia Conference on Information Systems: “Societal Transformation Through IS/IT”*, PACIS 2017. <http://aisel.aisnet.org/pacis2017/294>
- Slot, E. S. G. (2017). An approach for businesses to increase customer’s willingness to share personal information online s vase in the airline industry. *Master Thesis, Delft University of Technology*.
- Smailovic, V., Galetic, V., & Podobnik, V. (2013). Implicit social networking for mobile users: Data monetization for telcos through context-aware services. *Proceedings of the 12th International Conference on Telecommunications, ConTEL 2013*, 163–170.
- Snyman, J. H. (2021). Landlines, cellular, and internet protocol subscribership. *Journal of Strategic Innovation and Sustainability*, 16(4), 39–50. <https://doi.org/10.33423/jsis.v16i4.4620>
- Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, 154(3), 477–564. <https://doi.org/10.2307/40041279>
- Sujata, J., Sohag, S., Tanu, D., Chintan, D., Shubham, P., & Sumit, G. (2015). Impact of over the top (OTT) services on telecom service providers. *Indian Journal of Science and Technology*, 8(S4), 145. <https://doi.org/10.17485/ijst/2015/v8iS4/62238>
- Tanaiutchawoot, N., Bursac, N., Rapp, S., Albers, A., & Heimicke, J. (2019). Nudges: An assisted strategy for improving heuristic decision in PGE-product generation engineering. *Procedia CIRP*, 84, 820–825. <https://doi.org/10.1016/j.procir.2019.04.294>

- Tene, O., & Polonetsky, J. (2013). Big data for all: Privacy and user control in the age of analytics. *The Northwestern Journal of Technology and Intellectual Property*, 11(5), 1–36. <https://scholarlycommons.law.northwestern.edu/njtip/vol11/iss5/1>
- Terrel, S. R. (2016). *Writing a proposal for your dissertation*. The Guildford Press.
- The Radicati Group Inc. (2019). Mobile statistics report, 2019-2023. In *Statista* (Vol. 44, Issue 0). https://www.radicati.com/wp/wp-content/uploads/2019/01/Mobile_Statistics_Report,_2019-2023_Executive_Summary.pdf
- Thi, H., Nguyen, H., Le, A. Q., & Vu, H. Van. (2020). The impact of trust on personal information sharing. *IOSR Journal of Business and Management*, 22(4), 12–15. <https://doi.org/10.9790/487X-2204051215>
- Thunström, L., Gilbert, B., & Ritten, C. J. (2018). Nudges that hurt those already hurting – distributional and unintended effects of salience nudges. *Journal of Economic Behavior and Organization*, 153, 267–282. <https://doi.org/10.1016/j.jebo.2018.07.005>
- Tu, Z., Li, R., Li, Y., Wang, G., Wu, D., Hui, P., Su, L., & Jin, D. (2018). Your apps give you away. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 2(3), 1–23. <https://doi.org/10.1145/3264948>
- Tu, Z., Xu, F., Li, Y., Zhang, P., & Jin, D. (2018). A new privacy breach: User trajectory recovery from aggregated mobility data. *IEEE/ACM Transactions on Networking*, 26(3), 1446–1459. <https://doi.org/10.1109/TNET.2018.2829173>
- U.S. Senate Committee on Commerce, Science, and T. (2019). Policy principles for a federal data privacy framework in the United States. *Testimony before the Senate Committee on Commerce, Science, and Transportation*. <https://www.commerce.senate.gov/public/index.cfm/2019/2/policy-principles-for-a-federal-data-privacy-framework-in-the-united-states>
- Vainio, N., & Miettinen, S. (2015). Telecommunications data retention after Digital Rights Ireland: Legislative and judicial reactions in the Member States. *International Journal of Law and Information Technology*, 23(3), 290–309. <https://doi.org/10.1093/ijlit/eav010>
- Van Kleek, M., Liccardi, I., Binns, R., Zhao, J., Weitzner, D. J., & Shadbolt, N. (2017). Better the devil you know. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, 2017-May*, 5208–5220. <https://doi.org/10.1145/3025453.3025556>
- Vishwamitra, N., Li, Y., Wang, K., Hu, H., Caine, K., & Ahn, G. J. (2017). Towards PII-based multiparty access control for photo sharing in Online Social Networks. *Proceedings of ACM Symposium on Access Control Models and Technologies, SACMAT, Part F1286*, 155–166. <https://doi.org/10.1145/3078861.3078875>

- von Entreeß-Fürsteneck, M., Buchwald, A., & Urbach, N. (2019). Will I or will I not? Explaining the willingness to disclose personal self-tracking data to a health insurance company. *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 6, 1351–1361. <https://doi.org/10.24251/HICSS.2019.165>
- Wadle, L.-M., Martin, N., & Ziegler, D. (2019). Privacy and Personalization. *Adjunct Publication of the 27th Conference on User Modeling, Adaptation and Personalization, Haapie*, 319–324. <https://doi.org/10.1145/3314183.3323672>
- Wagner, I., & Eckhoff, D. (2018). Technical privacy metrics: A systematic survey. *ACM Computing Surveys*, 51(3), 1–38. <https://doi.org/10.1145/3168389>
- Waldman, A. E. (2016). Privacy, trust, and the propensity to disclose. *SSRN Electronic Journal*, 67(1). <https://doi.org/10.2139/ssrn.2726929>
- Wang, Y., Leon, P. G., Acquisti, A., Cranor, L. F., Forget, A., & Sadeh, N. (2014). A field trial of privacy nudges for facebook. *Proceedings of the 32nd Annual ACM Conference on Human Factors in Computing Systems - CHI '14*, 2367–2376. <https://doi.org/10.1145/2556288.2557413>
- Willis, L. E. (2013). Why not privacy by default? *SSRN Electronic Journal*, 61. <https://doi.org/10.2139/ssrn.2349766>
- Wills, C. E., & Tatar, C. (2012). Understanding what they do with what they know. *Proceedings of the 2012 ACM Workshop on Privacy in the Electronic Society - WPES '12*, 13. <https://doi.org/10.1145/2381966.2381969>
- Yadegari, M., & Gharaee, H. (2016). A novel network based privacy framework. *Proceedings of the 2016 8th International Symposium on Telecommunications (IST)*, 117–123. <https://doi.org/10.1109/ISTEL.2016.7881794>
- Yee, K.-P. (2005). Guidelines and strategies for secure interaction design. In *Security and Usability* (pp. 253--280).
- Yiakoumis, Y., Katti, S., & McKeown, N. (2016). Neutral net neutrality. *Proceedings of the 2016 ACM SIGCOMM Conference*, 483–496. <https://doi.org/10.1145/2934872.2934896>
- Yusoff, A. S. M., Peng, F. S., Razak, F. Z. A., & Mustafa, W. A. (2020). Discriminant validity assessment of eeligious teacher acceptance: The use of HTMT criterion. *Journal of Physics: Conference Series*, 1529(4), 0–7. <https://doi.org/10.1088/1742-6596/1529/4/042045>
- Zeng, F., Ye, Q., Li, J., & Yang, Z. (2020). Does self-disclosure matter? A dynamic two-stage perspective for the personalization-privacy paradox. *Journal of Business Research*, March 2019, 0–1. <https://doi.org/10.1016/j.jbusres.2020.02.006>

- Zhang, B., & Xu, H. (2016). Privacy Nudges for Mobile Applications. *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*, 27, 1676–1690. <https://doi.org/10.1145/2818048.2820073>
- Zhao, C., Hinds, P., & Gao, G. (2012). How and to whom people share: The role of culture in self-disclosure in online communities. *Proceedings of the ACM Conference on Computer Supported Cooperative Work, CSCW*, 67–76. <https://doi.org/10.1145/2145204.2145219>
- Zhao, P., Jiang, H., Lui, J. C. S., Wang, C., Zeng, F., Xiao, F., & Li, Z. (2018). P 3 - LOC: A Privacy-Preserving Paradigm-Driven Framework for Indoor Localization. *IEEE/ACM Transactions on Networking*, 26(6), 2856–2869. <https://doi.org/10.1109/TNET.2018.2879967>
- Zhou, T. (2012). Understanding users' initial trust in mobile banking: An elaboration likelihood perspective. *Computers in Human Behavior*, 28(4), 1518–1525. <https://doi.org/10.1016/j.chb.2012.03.021>
- Zulas, A. L., Crandall, A. S., & Schmitter-Edgecombe, M. (2014). Caregiver needs from elder care assistive smart homes: Children of elder adults assessment. *Proceedings of the Human Factors and Ergonomics Society, 2014-Janua(1)*, 634–638. <https://doi.org/10.1177/1541931214581150>