2021

The Influence of an Individual’s Disposition to Value Privacy in a Non-Contrived Study

John Marsh
Nova Southeastern University, mail@marshdom.com

The Influence of an Individual's Disposition to Value Privacy in a Non-Contrived Study

by

John Marsh

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

2020

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

Steven Zink

Steven Zink, Ph.D
Chairperson of Dissertation Committee

1/15/2021
Date

Gwendolyn Campbell

Gwendolyn Campbell, Ph.D.
Dissertation Committee Member

1/15/2021
Date

Ling Wang, Ph.D.
Dissertation Committee Member

1/15/2021
Date

Approved:

Meline Kevorkian

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

1/15/2021
Date

College of Computing and Engineering
Nova Southeastern University

2021

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

The Influence of an Individual’s Disposition to Value Privacy in a Non-Contrived Study

by
John E. Marsh
December 2020

Unexpected usage of user data has made headlines as both governments and commercial entities have encountered privacy-related issues. Like other social networking sites, LinkedIn provides users to restrict access to their information or allow for public viewing; information available in the public view was used unexpectedly (i.e., profiling). A non-profit entity called ICWATCH used tools to gather information on government mass surveillance programs by scraping publicly accessible user data from LinkedIn. Previous research has shown that privacy concerns influence behavior intention in contrived scenarios. What remains unclear is whether LinkedIn users, whose data was scraped by ICWATCH (an actual situation), would have similar privacy concerns and subsequently express the intent to take privacy-preserving action.

This study proposed to answer three research questions in the context of an actual privacy-centric situation, using an explanatory sequential mixed methods design. First, what is the user's disposition towards privacy? Second, to what extent does this influence users' privacy concerns regarding the inclusion of their LinkedIn profile information within ICWATCH? Third, to what extent do these concerns influence their stated intention to modify their LinkedIn profile/settings to minimize/eliminate this inclusion? The two-phase approach performed quantitative analysis on collected survey data, followed by analysis on follow-up interview data to provide context.

The resulting analyses found significant support for each hypothesis and divergence of underlying factors between degrees of the hypotheses and variable representations. Those participants who were not inclined to privacy and were not concerned with the situation, as expected, did not intend to modify their LinkedIn profile. However, they did express underlying factors such as control and privacy risk belief, unlike their counterparts. Those participants who were more inclined and more concerned about the situation did express an intent to modify their profile and revealed underlying factors such as regulations and usage. The findings support the extension of the existing literature onto actual privacy-centric situations. The results also highlight challenges with population demographics in actual situations and suggestions for construct prioritization when investigating future situations.

Acknowledgments

It has been a long 11-year journey, and I would like to take this opportunity to thank those who helped and supported me along the way. First, a tremendous thank you for the sacrifices in both effort and sanity made by my wonderful wife Marieliz, your contributions to this goal are too enumerable to list. You were there when I needed someone to push me forward, and I know there were times when the stress was nearly unbearable. You are a survivor and an inspiration.

Dr. Zink, who I am sure did not anticipate the chaos and slog he was inheriting nearly six years ago when he agreed to be my advisor. Thank you for being the voice of calm and reason as you mentored me through the chaos. Dr. Campbell, I am fortunate that our paths crossed, and I thank you for your ongoing friendship, guidance, and for volunteering to be part of this journey. Dr. Wang, thank you for serving on my committee and giving me the extra time to see this to completion. Each of you was instrumental in making this a reality.

Robert, I have been a student since you were born, and I know you were sick of hearing, "This paper doesn't write itself." While I tried to balance the load, I want to thank your past self for the sacrifices you unknowingly made. One day, I hope you will read this and not only sympathize with the stress of such an endeavor but be motivated to pursue your dreams.

Mom, I know you are proud and have been waiting for this moment for years; I made it!

Unfortunately, several family members who were there at the beginning were not with me at the end. Thank you for believing in me, and know that I wish you were here to see it Dad (John), Grandma (Olga), Roger (father-in-law), Nelly (mother-in-law), and Proctoy (brother-in-law).

Thank you to my validation team David, Eric, Rusty, and Scott. Also, a special thank you to all the individuals that volunteered to participate in my research. You took a chance on the plea from a student asking for help, and it made the difference. Finally, thank you for the ongoing words of encouragement from the rest of my family, friends, and colleagues (there are way too many to name); it gave me the strength to persevere.

Table of Contents

Appendices

List of Tables

Tables

List of Figures

Figures

Chapter 1

Introduction

Background

The availability of personal information on the Internet has broad implications as it relates to individual privacy. Dinev et al. (2008) note survey results where participants reveal that "Privacy is among the highest of individual rights," falling between freedom of speech and freedom of religion (p. 215). Warren and Brandeis (1890) defined privacy as the right to be left alone, which has been foundational for privacy research (Christin et al., 2011; Conger et al., 2013; Dinev et al., 2013; Miltgen & Peyrat-Guillard, 2014; Pavlou, 2011; Smith et al., 2011; Spiekermann & Cranor, 2009; Xu, Dinev et al., 2011). Building on this, Pavlou provides a consumer definition of privacy as the right not to be disturbed, and more specifically, not to have personal information used for purposes other than those for which the data was initially submitted. Concerns related to information privacy are increasingly prevalent due to the volume of information collected, transmitted, and stored by organizations (with and without consent), whose intentions are not always evident (Rusk, 2014; Schwaig et al., 2013). Pavlou notes that "Specifically, the tension between the proper use of personal information and information privacy has been touted as one of the most serious ethical debates of the information age" (p. 977). As Li et al. (2011) noted, privacy is a broad issue that poses particular problems for commercial entities. For example, data-dependent organizations such as Google, Facebook, and Amazon are particularly vulnerable to privacy-related concerns. Each has recently encountered privacy matters ranging from Facebook and Google's use of targeted raced-based advertising (Maheshwari & Isaac, 2016) or keywords (Miller, 2013), respectively, and Amazon's use of dynamic pricing purportedly based on customer data (Martinez, 2016). Miltgen and Smith (2015) note that, "Ironically, it appears that consumer concerns associated with surveillance, reported extensively during 2013 and 2014, are being directed more at commercial than government data interchanges" (p. 741).

Current research is replete with studies and polls highlighting opinions regarding various privacy concerns (PCON). Miltgen and Smith (2015) conducted polls indicating 70% of respondents expressing concerns regarding online tracking and profiling. Wakefield (2013) noted multiple surveys where 70-90% of respondents expressed concerns about privacy (i.e., increasing part of modern life, secondary use, access, and willingness to disclose). Bansal and Zahedi (2014) cite surveys where 93% of respondents were concerned about privacy in online transactions and other polls where two-thirds of United States citizens were concerned about the threat hackers and criminals posed to privacy. Recent studies have also noted privacy concerns related to online social networks (OSN). Jiang et al. (2013) reported that 33% of respondents were concerned about personal privacy loss in online social interactions. The user privacy concerns associated with social networking's situational aspects are explored in this research, explicitly that of user data being scraped from LinkedIn and posted to a third-party site (i.e., ICWATCH).

This research's relevant aspect is that user information shared with social media services is not limited to just that service. For instance, governments conduct or propose to conduct social media profiling for a variety of purposes, including vetting foreign nationals, vetting individuals for approval of security clearances (U.S. Office of the Director of National Intelligence [ODNI], 2016), criminal activity (Joy, 2016), and fraudulent welfare recipients (Farrell, 2016). Commercial entities also use consumer data from social media. A U.S. Federal Trade Commission (2014) report indicated that commercial entities use social media data to enhance activities such as marketing (direct, online, and analytics), risk mitigation (identify verification and fraud detection), and people search, often without consumer knowledge. Subsequently, private entities, such as ICWATCH, also use social media information for profiling. Specifically:

> ICWATCH is a project to collect and analyze resumes of people working in the intelligence community. People working for intelligence contractors, the military, and intelligence agencies frequently mention secret codewords and surveillance programs in public resumes. These resumes are useful for uncovering new surveillance programs, learning more about known codewords, identifying which companies help with which surveillance programs, examining trends in the intelligence community, and more. (ICWATCH Surveillance, 2015)

The researcher designed this study to investigate the level of an individual's disposition to value privacy (DTVP), how this influences situation-specific Internet privacy concerns (SIPC) related to the information being scraped and posted by a third-party from LinkedIn, and ultimately, how this disposition influences the user's behavioral intention (BITN) to modify their LinkedIn account settings.

Problem Statement

The effect of privacy concerns in actual OSN usage (or continued usage) is poorly understood. While the literature has clearly shown that users' privacy concerns will influence their intended behavior in contrived scenarios, some indicate that users often behave in ways not necessarily reflected in their stated privacy concerns and attitudes. Xu and Gupta (2009) note an ongoing disagreement relating to the predictive reliability of intention. Pavlou (2011) cites additional privacy complexities, including the lack of a unified concept of information privacy, as well as how, "The role of context shapes the meaning and conceptualization of information privacy" (p. 980). There is no support for whether the linkage between privacy concerns and behavior intention is congruent with actual privacy situations.

If an individual's behavior related to privacy concerns can be unpredictable, it is essential to understand why. Contributing factors encompass various constructs and theories used in the literature and privacy's contextual and paradoxical aspects. Privacy studies contain a variety of constructs, including computer anxiety (Osatuyi, 2015), disposition (Li, 2014), perceived anonymity (Jiang et al., 2013), privacy concerns (Jiang et al., 2013; Li & Unger, 2012; Mao & Zhang, 2013; Miltgen & Smith, 2015; Schwaig et al., 2013; Xu et al., 2012; Zhang et al., 2013), self-esteem (Schwaig et al., 2013), trust (Zhou, 2015), and website reputation (Li, 2014). Privacy studies have also employed numerous theories, including the big five personality model (Osatuyi, 2015), cognitive consistency theory (Wakefield, 2013), control agency perspective (Xu et al., 2012), innovation diffusion theory (Luo et al., 2013), justice theory (Zhou, 2011), privacy paradox (Wakefield, 2013; Xu, Luo, et al., 2011), prospect theory (Bansal & Zahedi, 2014), social contract (Li et al., 2011), technology acceptance model (TAM) (Mao & Zhang, 2013), theory of planned behavior (Benson et al., 2015), theory of reasoned action (TRA) (Bansal et al., 2016; Bensen et al., 2015), and utility theory (Bansal & Zahedi, 2014). However, there is little representation across these constructs and theories in an existing/actual situation; it is not clear if these are applicable in actuality.

Many studies have also explored the contextual and situational aspects of privacy and its paradoxical nature. Throughout the literature, specific websites establish the context (i.e., financial, health, social media, travel) (Bansal et al., 2016; Bansal et al. 2010; Li et al., 2011; Li, 2014; Wakefield et al., 2011; Xu, Divev et al., 2011), type of website (i.e., chat, health, social media) (Bansal et al., 2010; Benson et al., 2015; Osatuyi, 2015), and/or type of service (i.e., location-aware marketing; location-based services, mobile commerce, mobile office) (Luo et al., 2013; Mao & Zhang, 2013; Xu et al., 2012; Xu, Luo et al., 2011; Zhang et al., 2013). Manipulating elements through experimentation allows for assessing situational aspects (Kayhan & Davis, 2016; Li et al., 2011). Wakefield (2013) notes that "Marketing researchers have coined the term, 'privacy paradox,' to describe the consumer who is reluctant to provide personal information yet succumbs to organizational requests for personal data" (p. 159). Multiple studies have explored this phenomenon in a variety of settings, including e-commerce (Wakefield, 2013; Xu, Luo et al., 2011), financial (Xu, Dinev et al., 2011), healthcare (Xu, Dinev et al., 2011), news services (Li & Unger, 2012), and social networking (Xu, Dinev et al., 2011). However, as noted earlier, these approaches are not actual situations; all are missing the influence of reality.

The privacy problem continues to grow, "As the reliance on web-based systems for delivery of services increases, privacy concern related to disclosing various types of personal information online gains prominence" (Bansal et al., 2010, p. 146). Most recently, Facebook was sued for the improper access to the data of 87 million users by Cambridge Analytica (Balsamo & Liedtke, 2018), while Google was also fined $57 million due to improper disclosure of data collection across services (for personalized advertising) (Satariano, 2019). Hong and Thong (2013) note that, "The increase in digitalized personal information and advances in Internet technologies pose new challenges to consumers' information privacy" (p. 13). As noted by Dinev (2014), another contributing factor is the paradoxical behavior of people stating their concerns about privacy as they continue to share their personal information, which may be illustrated by Facebook's rise in daily active users over 2018 (Isaac, 2019). Complicating this further is a lack of clarity of the problem. As Bansal and Zahedi (2014) note, companies hesitate to disclose/share breach data due to potential business loss.

Goals

There were three goals for this research study. First, the research results will contribute to the literature by providing empirical justification for a relationship between privacy concerns and behavior intention in an actual privacy-centric situation. Second, the research will justify the appropriateness of the constructs regarding usage in an actual situation. Third, the research will also justify scales' suitability for assessing privacy concerns with an actual situation.

As defined in multiple reference studies, behavior intention is either an intention to disclose (Bansal et al., 2016; Cichy et al., 2014; Jiang et al., 2013; Li et al., 2011; Miltgen

& Peyrat-Guillard, 2014; Xu, 2010) or intention to use/continue using (Bansal et al., 2010; Ku et al., 2013; Li & Unger, 2012; Li, 2014; Mao & Zhang, 2013; Osatuyi, 2015; Schwaig et al., 2013; Zhang et al., 2013; Zhou, 2015, 2011). Numerous researchers have assessed privacy behaviors through experiment (Bansal et al., 2016; Li & Unger, 2012; Li et al., 2011) or observed behavior (Chakrabotry et al., 2013; Chen & Sharma, 2012; Jiang et al., 2013; Miltgen & Payrat-Guillard, 2014; Zhang et al., 2013). Nevertheless, a gap remains between intentions and actual vs. contrived scenarios. This gap merits further investigation, as Xu and Gupta (2009) note concerns in the predictive ability of stated intentions, drawing from the weak relationship between subjective (self-reported) and objective (actual) system usage that Straub et al. (1995) observed.

This research further extends the dimensions utilized by Xu et al. (2012), which denoted that, "Privacy concerns are context-specific, based in the specifics of by whom, why, when, and what type of personal information is being collected, distributed, and used" (p. 3) and can vary over time for the same person (Conger et al., 2013). Their research extended other research by Li et al. (2011), which posited that the effect of general privacy concerns might be less critical than situation-specific ones. The study contributed new insights into the situational elements of privacy concern by demonstrating its impact on behavior intentions related to a current privacy-centric social media situation.

While the hypotheses predict (a) a user's disposition towards privacy would influence their privacy concern regarding having their information scraped by ICWATCH and (b) would declare their intention to take steps to modify their profile to stop sharing the information, there were a variety of other possible outcomes, as noted in Table A1. As part of the research design, participants were divided into outcome groups so that interview responses could provide context into the varying degrees of support for each variable. However, only the two groups aligned with the full hypothesis support were well represented (OG-A and OG-H).

This research strengthened the usage of general privacy concern constructs for future research streams. The usage of general privacy concern constructs is well represented throughout the reference studies, but not in an actual, current privacy-centric situation. Multiple studies have used general privacy concern constructs to examine: contrived scenarios (Choi & Land, 2016; Kayhan & Davis, 2016), experience with the Internet (Dinev & Hart, 2006; Son & Kim, 2008), experience with a specific site (Min & Kim, 2015; Ozdemir et al., 2017; Xu, Dinev et al., 2011), and perceptions of a specific site (Li, 2014; Li et al., 2011). Where the constructs were lacking usage was in an actual (non-contrived) situation.

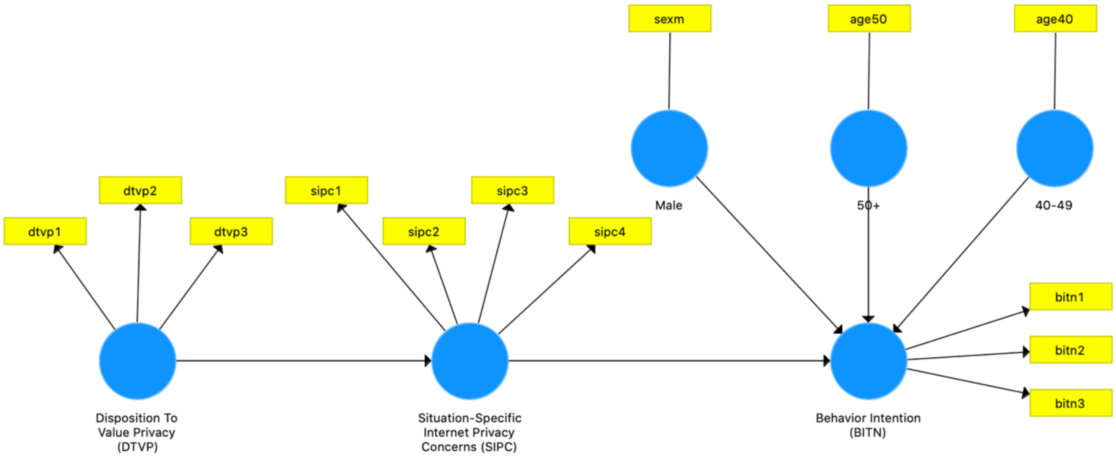
The research also encouraged increased use of scales for DTVP (aka general privacy concerns) and situational privacy concerns. Kayhan and Davis (2016) used existing scales for DTVP to study its influence on Internet privacy concerns via contrived scenarios. Others used similar techniques for examining experiences with a specific site (Xu, Dinev et al., 2011) and perceptions of a specific site (Li, 2014). Researchers also used the existing scales to evaluate situational privacy concerns and their influence on behavior via experience with the Internet (Dinev & Hart, 2006; Son & Kim, 2008) and experience with specific sites/services (Min & Kim, 2015; Ozdemir et al., 2017). Again, where the scales lacked usage was in a current and actual (non-contrived) situation.

Questions and Hypotheses

Studies by Kayhan and Davis (2016) and Li (2014) served as a basis for constructing the research framework for this study. As part of their research models, both studies evaluated the relationship between DTVP and contextual privacy concerns. Kayhan and Davis assessed the influence of DTVP on situational privacy concerns using contrived scenarios. Li evaluated the relationship between DTVP and site-specific privacy concerns. Li also investigated the relationship between site-specific privacy concerns and behavioral intention (i.e., privacy-preserving behavior). The research focused on evaluating three questions, supporting the simplified framework shown in Figure 1.

Figure 1

Research Model


sexm
age50
age40
Male
50+
40-49
dtvp1
dtvp2
dtvp3
sipc1
sipc2
sipc3
sipc4
bitn1
bitn2
bitn3
Disposition To Value Privacy (DTVP)
Situation-Specific Internet Privacy Concerns (SIPC)
Behavior Intention (BITN)

Note. As each of these control variables was categorical, each category was modeled as dummy (binary) variables; age used five dummy variables, and sex used two. Four dummy variables (30-39, 20-29, <20, and female) had insufficient analysis samples.

1. What is the user's disposition towards privacy (DTVP)?
2. What is the user's level of privacy concern regarding their information being scraped from LinkedIn and posted to ICWATCH (SIPC)?

3. To what extent do their concerns influence their intention to continue sharing information openly on LinkedIn (BITN)?

Disposition to Value Privacy (DTVP)

DTVP was also studied as a global information privacy concern (GIPC), and general privacy concern is a person's general attitude towards privacy. Researchers have variously defined DTVP as the desire/need for privacy (Li, 2014), tendency to worry about information privacy (Li et al., 2017; Li et al., 2011), tendency to preserve or restrain disclosure of private/personal information (Xu, Dinev et al., 2011), or the inherent worries about the opportunistic behaviors of providers (Kayhan & Davis, 2016). DTVP is not specific to any website or company (Li et al., 2017; Li et al., 2011) or specific contexts (Xu, Dinev et al., 2011). DTVP can differ among individuals (Li et al., 2011) and can influence situation-specific (Kayhan & Davis, 2016) and website-specific privacy concerns (Li, 2014).

Situation-Specific Internet Privacy Concern (SIPC)

Unlike DTVP, situation-specific Internet privacy concerns, also studied as Internet privacy concerns, are more specific than dispositional (Xu, Dinev et al., 2011). Xu, Dinev et al. define internet privacy concerns as an individual's anxiety resulting from privacy loss via information disclosure to a website. Others’ definitions focus on information flow via a website (Min & Kim, 2015), website or peer misuse of information (Ozdemir et al., 2017), effects of opportunistic behaviors related to submitted information (Dinev & Hart, 2006), or online companies’ practices and use of information (Son & Kim, 2008).

Research has demonstrated that DTVP positively affects internet privacy concerns (Kayhan & Davis, 2016; Li, 2014; Xu, Dinev et al., 2011). Researchers have used a variety of methodologies to establish this effect, including visiting a website followed by a survey (Li, 2014), a survey conditional on previous interaction with a type of website (Xu, Dinev et al., 2011), and a survey with contrived experiment scenarios (Kayhan & Davis, 2016). Kayhan and Davis also found that DTVP positively impacted situational privacy concerns in an experimental context manipulating privacy situations (e.g., presenting a privacy violation due to inadequate security measures). Considering the contiguous support for the positive relationship between DTVP and Internet privacy concerns, it should remain valid in an actual privacy-centric situation. Therefore, the first hypothesis is:

Hypothesis One (H1). Disposition to Value Privacy (DTVP) has a positive effect on situation-specific Internet privacy concerns (SIPC).

Behavioral Intention

Schwaig et al. (2013) note that privacy concerns influence a user's attitude towards a specific information practice and/or intention to use a system. Li (2012) suggests, “That an individual's intention to disclose information is based on the comparison of expected benefits and perceived risks in a given context” (p. 1). The relationship between privacy concern and behavior intention has been studied extensively in the literature. Specific examples of intentions influenced by Internet privacy concerns include willingness to provide personal information to transact on the Internet (Dinev & Hart, 2006), engage in privacy-protective responses (i.e., complain, refuse to participate, or falsify data) (Son &

Kim, 2008), and continuous intention to use social network services (SNS) (Min & Kim, 2015).

Numerous studies demonstrate that privacy concerns negatively affect intention to disclose/provide personal information (Bansal et al., 2010; Dinev & Hart, 2006; Dinev et al., 2008; Li et al., 2017; Li et al., 2011; Zhang et al., 2018; Min & Kim, 2015; Ozdemir et al., 2017) and use or continued use of a site or service (Ku et al., 2013; Li, 2014; Mao & Zhang, 2013; Schwaig et al., 2013; Xu, 2010). Research has also demonstrated that Internet privacy concern negatively affects behavior intention, established through the survey methodology (Dinev & Hart, 2006; Min & Kim, 2015; Son & Kim, 2008). Again, considering the contiguous support for the negative relationship between Internet privacy concerns and behavior intention, it should continue to remain valid in an existing situation. Therefore, the second hypothesis is:

Hypothesis Two (H2). Situation-specific Internet privacy concerns (SIPC) have a negative effect on the intention to continue sharing information publicly on LinkedIn (BITN).

Control Variables

This study used age and sex as the two control variables. Age was used in 91% of the reference studies and placed into the five most categories in the reference studies. Sex (also studied as gender) was used in 81% of the reference studies and evaluated as a binary variable.

Relevance

The relevance of this research rests on three factors. First, the research trends toward a more focused context (i.e., broad to specific). Second, the research focus is a problem that continues to grow as a growing body of users contribute data used in unforeseen ways. Finally, the literature shows that while privacy concerns influence intended behavior, it can also be influenced by other factors (e.g., benefits), neither of which can be sufficiently reliable without analysis of actuality analysis. The observed research trend in the context of privacy concern supports the relevance of this research. A review of the construct-aligned studies shows a clear trend from broad to specific in terms of online context, as described in Table 1. For example, one can see a trend starting with privacy concerns regarding the Internet (broad) to concerns interacting with Facebook (specific).

Table 1

Privacy Concern Research Focus

Focus	Years	Context	References
Broad ↓ Specific	2006-2008	Internet, Online Companies	Dinev & Hart, 2006; Dinev et al., 2008; Son & Kim, 2008
	2010-2014	Website Categories	Bansal et al., 2010; Li, 2014; Li et al., 2011; Li & Unger, 2012; Xu, Dinev et al., 2011
	2014-2017	Social Media, Facebook	Choi & Land, 2016; Ku et al., 2013; Li et al., 2017; Min & Kim, 2015; Osatuyi, 2015; Ozdemir et al., 2017

According to LinkedIn’s website (press.linkedin.com/about-linkedin), the service has more than 722 million users. According to the ICWATCH website (transparencytoolkit.org/project/icwatch), the system has scraped over 100,000 resumes from LinkedIn (and other sources). Suppose ICWATCH continues to add resumes at a similar rate. In that case, this could add several thousand more resumes each year, not including the possibility of continuous monitoring/updating of resumes already scraped, potentially exposing the data of hundreds of thousands of individuals. Külcü and Henkoğlu (2014) note,

> The main reason for the need to be conscious about the use of social networking sites and attaching importance to privacy is the misuse of personal information by social networking sites or the misuse of the viewable content by other users. (p. 761)

While research indicates that privacy concerns influence behavior, other research suggests that this behavior is subject to change by the perceived benefit resulting from sharing information, denoted as the privacy paradox (Xu, Luo et al., 2011). Constructs such as the privacy calculus (Li et al., 2011) or privacy tradeoff (Jiang et al., 2013) can assess this paradox. User privacy concerns can also be influenced by situational (Kayhan & Davis, 2016; Li, 2014) and contextual (Bansal et al., 2016; Xu et al., 2012) factors. Another factor contributing to the problem is what information social media users choose to share. Cichy et al. (2014) note that privacy may be viewed as a commodity, and users may be willing to disclose personal data for reciprocal benefits. However, Osatuyi (2015) notes, "Unlike on social media platforms, customers on e-commerce sites are not required to disclose their personal information to complete transactions" (p. 11). What users choose to share may also change over time, as Bansal et al. (2010) note:

> Prior experiences shape individuals' attitudes and form their dispositions with respect to a given context or circumstance. For example, painful memories from an incident of privacy invasion (such as online disclosure of social security

> information that had led to identity theft) could shape individuals' beliefs about their vulnerability in the online environment. (p. 146)

However, Li et al. (2011) note, "With progressive Web site interaction, the effect of general privacy concern will be gradually mediated or overridden by specific emotional and cognitive reactions to the Web site" (p. 442). This observed contradiction necessitates the need to evaluate privacy concerns in an actual privacy-centric situation.

Significance

This study is unique because it evaluated what participants declare they will do (well covered in literature) in the context of an actual privacy-centric situation (little coverage in literature). Relevant literature indicates that the influence of privacy concerns on behavior is generally evaluated in two ways: a participant's statements regarding their actions (Jiang et al., 2013; Miltgen & Peyrat-Guillard, 2014) and what the participant has stated they will do (intention) (Bansal et al., 2010, 2016; Dinev et al., 2008; Ku et al., 2013; Li et al., 2011; Li & Unger, 2012; Li, 2014; Mao & Zhang, 2013; Osatuyi, 2015; Schwaig et al., 2013; Xu, 2010; Xu & Gupta, 2009). It is also worth noting that other privacy-related studies have evaluated behavior (concerning general privacy) based on how users had previously acted (dataset reviews). The assumption for this lack of research based on real situations is due more to the difficulty in finding real-world situations than a lack of interest or oversight by the research community. Possible results from the research also contribute to the literature, regardless of support for the proposed hypotheses. As stated earlier, most of the outcomes will either strengthen or weaken the observed relationships between general and situation-specific privacy concerns and/or the relationship between situational privacy concerns and behavioral intention.

Barriers

Many factors contribute to the challenges of exploring privacy concerns and behavior. Opportunities to study real privacy-centric situations are problematic; service providers likely deem such research undesirable as it could provide an unfavorable view of their service. Given the limited opportunities for assessing real privacy-related situations, many studies substitute contrived scenarios and previous behaviors instead. Researchers employ a variety of methods to assess behavioral intention, including fabricating websites for assessment (Li et al., 2011), scenarios (Cichy et al., 2014; Li & Unger, 2012), assessing general privacy beliefs (Miltgen & Peyrat-Gillard, 2014; Schwaig et al., 2013), review existing websites (Bansal et al., 2016), and assessing services (e.g., chat, LBS, m-commerce, and social media) (Jiang et al., 2013; Ku et al., 2013; Li, 2014; Mao & Zhang, 2013; Osatuyi, 2015; Zhou, 2011). However, each of these has only yielded a prediction of the individual's actual behavior in a contrived scenario. Underlying this, as noted by Schwaig et al. (2013), many assume that users behave rationally.

During 2018, LinkedIn changed its website access and set up an authorization wall, making it challenging to correlate which users listed on ICWATCH were still publicly sharing their profile via LinkedIn. Complicating this further, LinkedIn public profile setting modifications may also take weeks to propagate through search engines. These barriers made an evaluation of actual behavior, in the context of this study problematic; authorized users always have full profile access. Future modifications to the underlying services were a concern throughout the study.

Issues

Several issues were associated with the research study. First, the literature has demonstrated that multiple variables can influence privacy concerns and behavior or moderate their relationship. Next, the potential for an interaction effect existed based on the methodology selected. Lastly, there were also potential issues with the selection of a convenience population.

Many studies have examined the direct link between privacy concerns and behavioral intention (Bansal et al., 2016; Ku et al., 2013; Li & Unger, 2012; Li et al., 2011; Li, 2014; Mao & Zhang, 2013; Miltgen & Peyrat-Guillard, 2014; Osatuyi, 2015; Schwaig et al., 2013; Zhang et al., 2013). Still, other studies suggest numerous additional variables influence each factor independently and/or moderate the relationship between the two. Other variables influencing behavior include attitude (Chen, 2013a; Chen & Sharma, 2015; Schwaig et al., 2013), computer anxiety (Osatuyi, 2015; Schwaig et al., 2013), control (Benson et al., 2015), enjoyment (Chen, 2013b), perceived benefits (Li, 2014), perceived rewards (Miltgen & Smith, 2015), privacy protection beliefs (Li et al., 2011), privacy risk (Chen, 2013b; Li et al., 2011; Luo et al., 2013; Zhou, 2011, 2015), self-esteem (Schwaig et al., 2013), technology acceptance factors (Mao & Zhang, 2013; Zhou, 2015), trust (Bansal et al., 2016; Chen & Sharma, 2012; Treiblmaier & Chong, 2011; Wakefield, 2013; Zhou, 2011, 2015), and use (Benson et al., 2015). Other variables influencing privacy concerns include: hyper-personal framework aspects (Jiang et al., 2013), information sensitivity (Kayhan & Davis, 2016), perceived control (Xu et al., 2012), personality traits (Osatuyi, 2015), previous online privacy invasion (Bansal et al., 2016), regulatory protection (Miltgen & Smith, 2015), trust (Miltgen & Smith, 2015), website familiarity (Li, 2014), and website reputation (Li, 2014). Variables moderating the relationship between privacy concern and behavior include geographic region (Ku et al., 2013), industry domain (Li & Unger, 2012), experience (Li & Unger, 2012), perceived quality of personalization (Li & Unger, 2012), perceived rewards (Miltgen & Smith, 2015), and trust (Cichy et al., 2014). Another factor contributing to the complexity of the issue is the contextual nature of privacy. Li et al. (2011) note:

> In comparison, general privacy concern was found to be a far less important factor influencing privacy beliefs and behaviors. The results not only provide important insights into resolving some of the equivocation found in the literature regarding privacy behavior, but also better explain inconsistencies in consumers' privacy behavior found in practice. (p. 435)

Studies have also noted situational and contextual factors that may override general privacy concerns (Li et al., 2011; Xu et al., 2010) via numerous contextual factors influencing privacy concerns, including information contingency, privacy interventions, and requesting organizations (Miltgen & Peyrat-Guillard, 2014).

Considering this, some interaction effects may have skewed the research results or potentially disqualified participants prematurely. The author assumed that most participants were unaware of the situation. Making them aware of it in the survey introduction could have prompted premature (regarding this study) privacy-preserving behavior. Users may have chosen not to participate based on this action or disqualified themselves despite the wording of the disqualifying question on the questionnaire.

This study’s proposed convenience population was comprised of individuals associated with the intelligence community per the ICWATCH website and are 1st- or

2nd-degree LinkedIn connections to the author. The population may be a source of potential sample bias, considering the LinkedIn relationship with the author and the LinkedIn limitations on the total number of results in any given search. However, these users were part of the larger population (all LinkedIn users included within ICWATCH). The use of a convenience population does not necessarily limit the results' generalizability, as Li et al. (2010) noted. Several of the reference studies have utilized convenience populations, especially among student populations (Bansal et al., 2010, 2016; Jiang et al., 2013; Li et al., 2011; Mao & Zhang, 2013; Osatuyi, 2015; Xu, 2010; Zhang et al., 2013).

Assumptions

The research made several assumptions. First, users were not aware of this situation; however, it is conceivable that they were. As noted earlier, the literature has observed a privacy paradox (Wakefield, 2013; Xu, Luo et al., 2011), where the perceived benefit of the service overrides the user's privacy concerns. It is reasonable to assume that users may make their LinkedIn profiles available to be discovered and that a situation such as this was conceivable.

Second, that it was appropriate to continue evaluating privacy concerns as a unidimensional construct. Literature addressing privacy concerns' influence on intended behavior as a unidimensional construct is plentiful. However, privacy concerns influencing intended behavior is also well represented as a multidimensional construct. The researcher assumed that a unidimensional approach to evaluate "real situation" privacy concerns was appropriate in that it provided a foundation for future multidimensional evaluation.

The proposed focus qualified as a privacy-centric situation. Modeling the elements of the Facebook/Cambridge Analytica situation described earlier, it would appear that this situation involves (a) users voluntarily providing information to one company, while (b) a second company was using that data without consent. While this situation may be similar in those elements, other elements such as the discretionary LinkedIn profile visibility settings and the unassociated third-party relationship between LinkedIn and ICWATCH may invalidate this assumption.

Limitations

There were two identified limitations associated with the research, the reliance on external services, and the social media privacy environment. This study relied on external services (LinkedIn and ICWATCH), specifically their availability and behavior. As discussed earlier, LinkedIn changed its website access forcing a modification to the methodology. The security update only illustrates that any alterations to either service would have dramatically affected this research. Second, any newsworthy privacy event could have influenced people's perceptions of privacy regarding this situation. As noted earlier regarding Facebook and Cambridge Analytica, a similar privacy situation with Microsoft or LinkedIn (for example) could temporarily contribute to anomalous results. While participants may not have expressed any concern regarding LinkedIn and ICWATCH situation, they may have conflated a more recent event with this situation, thereby skewing the results.

Delimitations

The author created specific options limiting decisions to constrain this study's scope, including the number of privacy-preserving behaviors, the number of control variables, population exclusions, and time horizons. First, the only privacy-preserving behavior within this study’s scope was modifying "Your profile's public visibility" of the user's LinkedIn profile. It is reasonable to assume that a savvy user would understand that their profile data could be modified to remove intelligence community participation indicators (i.e., codewords or other terms) as an alternative privacy-preserving behavior. However, given the breadth of potential indicators for ICWATCH to monitor, it would be imprudent to imply that this is appropriate protection for the participant. The author also controlled only two variables (age and sex) for inclusion due to their representation in the reference studies and implemented an arbitrary 80% cutoff to limit the scope. While there were several other relevant control variables such as experience (31% of reference), usage (46% of reference), and education (31% of reference), they had notably less representation in the literature.

As noted earlier, this study used 1st- and 2nd-degree connections as part of the target population, which permitted the inclusion of the "Introduction" feature (i.e., via first connections). Expanding the population to include 3rd-degree connections would have limited the study to only using the "Connect" function within LinkedIn. Upon completing the quantitative analysis, the author chose willing participants selected from groups aligned with the outcomes described in Table 1. The researcher conducted follow-up interviews on participants in groups meeting a 5% sample representation threshold to provide context to the survey results.

Finally, the LinkedIn website states, "After you change or disable your profile public [sic], it may take several weeks for it to be added to or removed from search engine results" (www.linkedin.com/help/linkedin/answer/83/linkedin-public-profile-visibility?lang=en). To allow for this possibility, the questionnaire included a suitability question asking if the respondent had modified "Your profile's public visibility" within the last 30 days, via LinkedIn "Settings and Privacy" options for any reason other than due to your profile information being on ICWATCH? The author allowed 30 days to pass to permit search engines to update and to place the time in context (approx. one month) for ease of user perception. However, there is no guarantee that users who modified their profile 30 days earlier would still not be visible via search engines.

Definition of Terms

Table 2 provides a list of terms and their associated definitions found throughout the research proposal.

Table 2

Definition of Terms

Term	Definition	References
1st-degree connection	Within the LinkedIn network, 1st-degree connections have accepted an invitation to connect to another member.	LinkedIn, 2019
2nd-degree connection	Within the LinkedIn network, 2nd-degree connections are other members connected to a user's 1st-degree connection(s) (i.e., no direct connection).	LinkedIn, 2019
3rd-degree connection	Within the LinkedIn network, 3rd-degree connections are other 1st degree connections with a user's 2nd-degree connection.	LinkedIn, 2019

(continued)

Term	Definition	References
behavior intention	The intention of a LinkedIn user to continue to share their LinkedIn profile publicly.	Li, 2014; Li et al., 2011; Osatuyi, 2015; Schwaig et al., 2013; Zhou, 2011
disposition to value privacy	A person's general attitude towards privacy.	Kayhan & Davis, 2016; Li, 2014; Li et al., 2011; Li et al., 2017; Xu, Dinev et al., 2011
ICWATCH	A project, hosted by WikiLeaks that collects and analyzes resumes from various social networks to identify people working in the intelligence community and make them searchable through a software solution called LookingGlass.	ICWATCH Surveillance, 2015
privacy concern	An individual's concerns resulting from the loss of privacy from information disclosure to a website, flow of information with a website, or misuse of information by a website or peers, effects of opportunistic behaviors related to submitted information, and practices and use of information by online companies.	Dinev & Hart, 2006; Min & Kim, 2015; Ozdemir et al., 2017; Son & Kim, 2008; Xu, Dinev et al., 2011
privacy paradox	The contradiction arising from a user’s stated privacy concern and their actual behavior.	Li & Unger, 2012; Wakefield, 2013; Xu, Luo et al., 2011

List of Acronyms

Table 3 provides a list of acronyms found throughout the research proposal.

Table 3

List of Acronyms

Acronym	Term
AVE	average variance extracted
BEHV	Behavior
BITN	behavior intention
BNFT	Benefit
CFIP	concern for information privacy
CMB	common method bias
CNTL	Control
COLL	Collection
CR	composite reliability
DTVP	disposition to value privacy
e-commerce	electronic commerce
ERRS	Errors
FTC	Federal Trade Commission
GIPC	global information privacy concern
GPCN	general privacy concern
ICWATCH	intelligence community watch
INVN	Invasion
IS	information system
IUIPC	Internet user's information privacy concern
m-commerce	mobile commerce
MPEG	moving picture experts group
OG-	outcome group
ODNI	Office of the Director of National Intelligence
OSN	online social network
P1	phase one

(continued)

Acronym	Term
P2	phase two
PCON	privacy concern
PLS	partial least squares
PLSc	consistent PLS algorithm
PNTR	personality traits
PRBF	privacy risk beliefs
REGL	Regulation
SEM	structural equation modeling
SIGINT	signals intelligence
SIPC	situation-specific Internet privacy concern
SPCN	specific privacy concerns
TAM	technology acceptance model
TPB	theory of planned behavior
TRA	theory of reasoned action
USGE	Usage

Summary

This chapter provided background regarding the ongoing problem of privacy as it relates to social media. Current research lacks visibility into real privacy-centric situations. This study's goals were identified as contributing to the existing literature, appropriateness of constructs, and the use of scales to assess “real-world” privacy-centric scenarios. The author presented two research hypotheses to evaluate the influence of DTVP on situational privacy concerns and, subsequently, situational privacy concerns on privacy-preserving behaviors. Much of the study's significance is its unique approach to evaluating an actual privacy-centric situation, not presently represented in the literature. The author outlined barriers associated with exploring real privacy situations and possible variable quantity and interaction effects. The author also introduced assumptions regarding the research proposal (i.e., cognition, dimensionality, applicability). Finally, limitations such as the reliance on external services and delimitations such as imposed restrictions on population and time were enumerated.

Chapter 2

Review of Literature

Constructs and Theories

This study evaluates the influence of DTVP (aka general privacy concern) on situational privacy concerns and situational privacy on behavioral intention (e.g., privacy-preserving). The literature on these relationships offers a variety of frameworks and theories. However, researchers have generally only evaluated these relationships in a notional or contrived context. This study proposes to explore the relationships in the context of an actual privacy-centric situation.

Privacy Concern

Of the variety of constructs used within information systems (IS) research (e.g., experience, risk, security, sensitivity, usage, and trust), privacy concern has been one of the most widely used (Li et al., 2010; Xu & Gupta, 2009), with the most inconsistent results (Li et al., 2010). Privacy concern generically can be defined as reflecting a user's concern (or worry) about personal information regarding its collection, storage, and use (Xu & Gupta, 2009; Zhou, 2015). Collection concerns include factors such as methodology, time, and disclosure. Concerns regarding the storage of personal information include factors such as amount, accuracy, and access protections. Usage concerns include factors such as inappropriate/undisclosed applications (e.g., discrimination and marketing) and sharing (Hui et al., 2007; Kobsa, 2007).

Researchers have widely studied privacy concerns in a general context. Li et al. (2011) noted,

> A large body of research has focused on consumers' general privacy concern, which is defined as an individual's general tendency to worry about information privacy. General privacy concern is not specific to a particular context (e.g., a specific Web site or online company) and differs from person to person. (p. 434)

Xu et al. (2012) also support this view regarding a detailed study of general privacy concerns.

Researchers have also examined privacy concerns as both a unidimensional and multidimensional construct. From a unidimensional approach, privacy concerns have generated numerous studies related to its influence on a variety of constructs, including behavior intention (Dinev et al., 2008; Li, 2014; Li et al., 2017; Li et al., 2011), control (Xu, Dinev et al., 2011), privacy risk belief (Li et al., 2011; Xu, Dinev et al., 2011), specific privacy concern (Kayhan & Davis, 2016; Li, 2014), and trust (Bansal et al., 2010). Information sensitivity also influences general privacy concerns (Bansal et al., 2010) and privacy experience (Li, 2014). Smith et al. (1996) note that “it is common for information privacy to be approached as though it were a unidimensional construct” (p. 169) and studied as a general privacy concern or DTVP (Kayhan & Davis, 2016; Li, 2014; Li et al., 2017; Li et al., 2011; Xu, Dinev et al., 2011).

Smith et al. (1996) developed a scale to measure multidimensional privacy concerns, which has been used and adapted in recent research (Mao & Zhang, 2013; Osatuyi, 2015;

Smith et al., 1996; Stewart & Segars, 2002; Xu, 2010; Xu & Gupta, 2009; Xu et al., 2012; Zhang et al., 2013; Zhou, 2011) and is often referred to as concerns for information privacy (CFIP). CFIP encompasses four dimensions: collection (the amount of data accumulated/stored), errors (deliberate or accidental inaccuracies), unauthorized secondary use (internal and external, collected for one purpose but used for another), and improper access (availability to unauthorized people). Malhotra et al. (2004) later extended this to the Internet users' information privacy concerns (IUIPC), which encompasses three factors: collection, control, and awareness of privacy factors. Jiang et al. (2013) have incorporated the IUIPC construct into current research.

Though generally not a primary focus, researchers have examined privacy concerns in contextual and situational conditions. While many studies have approached evaluating privacy in a general context, each study typically contained a specific contextual element, including location-based services (Zhou, 2015), online (Miltgen & Peyrat-Guillard, 2014), regulations (Miltgen & Smith, 2015), social media (Jiang et al., 2013; Ku et al., 2013; Osatuyi, 2015), and websites-general (Bansal et al., 2016; Kayhan & Davis, 2016). Multiple constructs have been studied regarding their influence from, upon, and moderating privacy concern within a contextual condition, including age (Zhang et al., 2013) behavior (Bansal et al., 2010; Dinev et al., 2008; Li, 2014; Xu, 2010), control (Xu, 2010; Xu et al., 2012), device (Xu, 2010), education (Zhang et al., 2013), experience (Zhang et al., 2013), familiarity (Li, 2014), gender (Zhang et al., 2013), income (Zhang et al., 2013), invasion (Bansal et al., 2010; Dinev et al., 2008), regulation (Xu, 2010), reputation (Li, 2014), risk (Zhou, 2011), sensitivity (Bansal et al., 2010), surveillance (Dinev et al., 2008), and trust (Bansal et al., 2010; Zhou, 2011). Several constructs have also been studied regarding their influence from, upon, and moderating privacy concerns within a situational condition, including behavior (Li et al., 2011), protection (Li et al., 2011), responsibility (Kayhan & Davis, 2016), risk (Li et al., 2011), and sensitivity (Kayhan & Davis, 2016).

Behavior/Intention to Disclose

Mackenzie and Spreng (1992) utilized a scale for measuring purchase intention, which had an implied definition of the likelihood to purchase an advertised product as influenced by attitude. Later, Jarvenpaa et al. (1999) and Jarvenpaa et al. (2000) expanded the construct into a willingness to buy. More recent studies have evolved the definition further, as Li et al. (2011) also utilized behavior intention (as modeled in this research) and described this as "The effect of salient privacy beliefs on intention to release personal information" (p. 438). Zhou (2011) used a similar construct, termed usage intention, which, "Reflect the usage, personal information disclosure and recommendation [of a service provider to others]" (p. 217). Other studies have used this construct as the intention to create online accounts (Osatuyi, 2015), use a site for inquiry (Li, 2014), create online accounts (Osatuyi, 2015), and use a site for information request (e.g., auction, financial, or travel) (Li, 2014). Schwaig et al. (2013) note that privacy concerns influence a user's attitude towards a specific information practice and/or intention to use a system. Li (2012) suggests, "That an individual's intention to disclose information is based on the comparison of expected benefits and perceived risks in a given context" (p. 1).

The literature reflects 42 factors that have been studied related to privacy regarding their influence on intention. However, only 10 were used in more than one study, including attitude (Mackenzie & Spreng, 1992; Schwaig et al., 2013), experience (Bansal et al., 2010, 2016), innovativeness (Xu & Gupta, 2009; Xu, Luo et al., 2011), privacy concern (Bansal et al., 2010, 2016; Dinev et al., 2008; Ku et al., 2013; Li et al., 2011; Li & Unger, 2012; Li, 2014; Mao & Zhang, 2013; Osatuyi, 2015; Schwaig et al., 2013; Xu, 2010;, Xu & Gupta, 2009), protection (Li et al., 2010, 2011; Li & Unger, 2012), risk (Li et al., 2010, 2011; Luo et al., 2013; Treiblmaier & Chong, 2011; Zhou, 2011, 2015), trust (Bansal et al., 2010, 2016; Treiblmaier & Chong, 2011; Wakefield, 2013; Zhou, 2011, 2015), usage (Li & Unger, 2012; Mao & Zhang, 2013), usefulness (Li et al., 2010; Luo et al., 2013; Mao & Zhang, 2013; Zhou, 2015), and value (Mao & Zhang, 2013; Xu, Luo et al., 2011).

Theories Associated with Privacy Concern

Li (2012) provided an integrated framework for privacy concern research theories and categorized them based on origin, consequences, trade-offs, and influential factors (institutional and individual). Table A2 provides an overview of this framework and a breakout of the theories used across the construct-aligned studies

The scales-aligned studies represented coverage across four categories, including consequence factors (Dinev & Hart, 2006), trade-off factors (Li, 2014; Li et al., 2011; Min & Kim, 2015), and institutional influential factors (Xu, Dinev et al., 2011). Expanding outward, the construct-aligned studies represented coverage across four categories, including origin factors (Li et al., 2010; Xu, 2010), consequence factors (Bansal et al., 2016; Dinev & Hart, 2006), trade-off factors (Bansal et al., 2010; Bansal et al., 2016; Dinev et al., 2008; Li, 2014; Li et al., 2011; Min & Kim, 2015), and individual influential factors (Choi & Land, 2016; Zhang et al., 2018). Finally, the construct-aligned studies with a contextual and situational focus covered three categories, including origin factors (Xu, 2010), trade-off factors (Bansal et al., 2010; Dinev et al., 2008; Li et al., 2011), and individual influential factors (Li, 2014).

Inclusions

The two constructs included in this research are unidimensional privacy concerns and behavior as intention. Multiple studies have identified a conflict in an individual's privacy concerns and subsequent behaviors (Joinson et al., 2010; Li et al., 2011; Zhou, 2011). Cichy et al. (2014) note that "Privacy concerns emerged as the most frequently mentioned factor affecting respondents' personal driving data disclosure intentions" (p. 6). Privacy concerns were also studied to observe their influence on "… Various behavior-related variables, e.g., willingness to disclose personal information, intention to transact, and information disclosure behavior" (Xu & Gupta, 2009, p. 140). Privacy concerns also constitute one of the most likely behavior-related variables to cause stress. As a general construct, privacy concern is well represented in the literature. Consistently, across several studies, DTVP demonstrated its influence on privacy concerns (Kayhan & Davis, 2016; Li, 2014; Xu, Dinev et al., 2011). Internet privacy concern (as a general construct) influencing behavior intention is also well supported in the literature (Dinev & Hart, 2006; Li et al., 2011; Li et al., 2017; Min & Kim, 2015; Ozdemir et al., 2017; Son & Kim, 2008).

As stated earlier, privacy concerns influence a user's attitude towards a specific information practice and/or intention to use a system (Schwaig et al., 2013). Li et al.'s (2011) work support this, noting, "Since the online consumer acts on beliefs and dispositions rather than solely on known costs and benefits, these beliefs factor into the privacy-related cost-benefit analysis" (p. 42). Several research lines also found trust influences a user's privacy concern and behavior (Joinson et al., 2010; Li et al., 2011; Xu et al., 2012; Zhou 2011, 2015). Additionally, Zhou (2015) notes that privacy concerns significantly affect privacy risk (uncertainty). Concurrently, for various reasons, users often behave in ways that do not reflect their privacy concerns and attitudes. For instance, users may sacrifice privacy for benefits they value (e.g., economic rationale). In other words, "Regardless of a user's expressed privacy concerns, they are willing to reveal the most intimate details of their personal preferences if deemed appropriate" (Spiekermann & Cranor, 2009, p. 71). A user's behavior is also not static. Their attitudes may change over time (Conger et al., 2013), influenced by the immediate benefits resulting from the disclosure over long-term privacy maintenance (Spiekermann & Cranor, 2009).

Exclusions

Multiple variants of privacy concern and behavior constructs, other related variables, and all of the theories related to privacy concern from the reference studies are excluded from this research. As noted earlier, two constructs for multidimensional privacy concern (CFIP and IUIPC) are also excluded. While both the influence of CFIP and IUIPC on behaviors are represented abundantly throughout the literature (Choi & Land, 2016; Mao & Zhang, 2013; Ostauyi, 2015; Xu, 2010; Xu & Gupta, 2009) with consistent results, neither has been studied in an existing privacy-centric situation. It was prudent to establish the validity of general privacy concerns before exploring multidimensional aspects.

The literature shows that privacy research behavior has also been modeled as prior action (via observation or dataset review) and prior stated action (conduct). Li et al.

(2015) used data collected from social networking sites to evaluate actual prior action against factors such as demographics, experience, network size, and productivity. The literature also notes 11 factors influencing conduct, including affiliation (Chen & Sharma, 2012), age (Chakraborty et al., 2013; Zhang et al., 2013), attitude (Chen, 2013a), enjoyment (Chen, 2013b), gender (Chakraborty et al., 2013), privacy concern (Jiang et al., 2013; Miltgen & Peyrat-Guillard, 2014), reciprocity (Chen & Sharma, 2012), reward (Jiang et al., 2013), risk (Chen, 2013b), trust (Chen & Sharma, 2012), and usage (Chen & Sharma, 2012). However, the researcher excluded both prior action and conduct as neither reflected intention in an actual privacy-centric situation, past vs. present application.

Privacy concern has been widely studied for its influence in a variety of constructs, including anonymity of others (Jiang et al., 2013), anonymity of self (Jiang et al., 2013), behavior (Bansal et al., 2016; Cichy et al., 2014; Jiang et al., 2013; Li et al., 2011; Li & Unger, 2012; Li, 2014; Osatuyi, 2015), computer anxiety (Osatuyi, 2015), disposition (Li, 2014), perceived intrusiveness (Jiang et al., 2013), perceived rewards (Miltgen & Smith, 2015), perceived usefulness (Zhou, 2015), personality traits (Bansal et al., 2016), personalization quality (Li & Unger, 2012), privacy protection belief (Li et al., 2011), privacy risk belief (Li et al., 2011; Zhou, 2015), psychological ownership (Cichy et al., 2014), trade-off discount (Bansal & Zahedi, 2014), trust (Cichy et al., 2014; Zhou, 2015), and website reputation (Li, 2014). Privacy concern has been regularly examined regarding its impact on other constructs, including behavior/adoption intention (Mao & Zhang, 2013; Osatuyi, 2015; Schwaig et al., 2013), computer alienation (Schwaig et al., 2013), computer anxiety (Osatuyi, 2015; Schwaig et al., 2013), control variables (i.e., age, education, experience, and income level) (Zhang et al., 2013), overall privacy concern (Mao & Zhang, 2013), perceived risk (Zhou, 2011), personality traits (Osatuyi, 2015), self-esteem (Schwaig et al., 2013), and trust (Zhou, 2011). Given that this study's focus was to validate the influence of general privacy concerns in an actual privacy-centric situation, all of these were excluded.

Extensive research shows that behavior influences and moderates other factors, such as privacy concerns (Li & Unger, 2012), protection (Li & Unger, 2012), and quality (Li & Unger, 2012). Researchers found moderating influence of behavior ranging from innovativeness (Xu & Gupta, 2009), motivation (Mackenzie & Spreng, 1992), privacy concern (Cichy et al., 2014; Ku et al., 2013; Osatuyi, 2015), quality (Li & Unger, 2012), and region (Ku et al., 2013) to relevance (Li et al., 2010), risk (Gerlach et al., 2015), sensitivity (Bansal et al., 2016), and value (Li & Unger, 2012). Again, as the research focus for this paper was to validate the influence of general privacy concerns on behavior intention in a real privacy-centric situation, all of these were excluded from examination.

Finally, all theories related to privacy concerns were excluded from this research. The research focused on establishing the influence validity of general privacy concerns on behavioral intention in an actual privacy-centric situation. The study did not seek to validate why it merely sought to provide context. Each of the theories required other constructs (e.g., beliefs and attitudes). As with all other privacy-related constructs, the study excluded all associated theories from the study.

Strengths

The literature's strength is the consistent results from the utilized scales, constructs, and methodologies. The scales-aligned studies found consistent results using the same measurement items for both DTVP and privacy concerns. Three studies found that DTVP positively affects privacy concerns, using the same items for DTVP (Kayhan & Davis, 2016; Li, 2014; Xu, Dinev et al., 2011). Three additional studies found that privacy concern negatively affects behavior intention, using the same items for privacy concern (Dinev & Hart, 2006; Min & Kim, 2015; Ozdemir et al., 2017).

The scales-aligned studies have also found consistent results using the same unidimensional approach for both DTVP and privacy concerns. Kayhan and Davis (2016), Li (2014), and Xu, Dinev et al. (2011) each found that unidimensional privacy concern constructs positively affected privacy concerns. Five studies found that unidimensional privacy concerns negatively affected behavior intention (Bansal et al., 2010; Dinev et al., 2008; Li et al., 2011; Li, 2014; Li et al., 2017. Finally, 10 of the reference studies found consistent results investigating the influence of privacy concern (both uni and multidimensional) using a survey methodology, demonstrating that privacy concerns' negative effect on behavior intention (Dinev et al., 2008; Dinev & Hart, 2006; Ku et al., 2013; Mao & Zhang, 2013; Min & Kim, 2015; Osatuyi, 2015; Ozdemir et al., 2017; Son & Kim, 2008; Xu & Gupta, 2009; Zhang et al., 2018).

Weakness/Gaps

Identified weaknesses amongst the reference studies included minimal investigation into situational influences associated with privacy concerns and behavior and research focused on actual situations. As previously discussed, researchers have noted that situational and contextual factors can influence privacy concerns (Kayhan & Davis, 2016; Li et al., 2011; Xu et al., 2010). However, limited studies have focused on the contextual and situational elements of privacy concern, with only four of the reference studies having a contextual focus (Bansal et al., 2010; Dinev et al., 2008; Li, 2014; Xu, 2010) and only two having a situational focus (Kayhan & Davis, 2016; Li et al., 2011).

The literature is also limited in investigations using existing privacy-centric situations. Ten of the reference studies investigated privacy concern's influence on behavior intention based on a user's experience, including experience with the Internet (Dinev et al., 2008; Dinev & Hart, 2006; Son & Kim, 2008), experience with the type of site/service (Ku et al., 2013; Mao & Zhang, 2013; Osatuyi, 2015; Xu, Dinev et al., 2011; Zhang et al., 2018), and experience with specific site/service (Min & Kim, 2015; Ozdemir et al., 2017). Three studies evaluated a user's perceptions of a specific site, both real and contrived (Bansal et al., 2010; Bansal et al., 2016; Li, 2014; Li et al., 2011; Xu, 2010; Xu & Gupta, 2009). Four studies have utilized privacy scenarios (Choi & Land, 2016; Gu et al., 2017; Li & Unger, 2012; Kayhan & Davis, 2016). Finally, four studies evaluated privacy concern and/or privacy behavior from a historical approach, either demonstrated action (via observation or dataset review) (Chakraborty et al., 2013; Li et al., 2015) or stated action (conduct) (Jiang et al., 2013; Miltgen & Peyrat-Guillard, 2014).

Similar Study Methods

While 31 of the reference studies contained at least one hypothesis related to privacy concerns, only 21 had similar construct assessments and/or utilized the same scales. Those were studies examining the relationship of dispositional privacy concerns and site/situation-specific privacy concerns (3), those that studied the relationship between privacy concerns and behavior intention (19), and those utilizing the same scales (9). Table 4 provides a breakout of these studies.

Table 4

Reference Studies Alignment Matrix

Area of Alignment	Reference Studies	Overlap Utilizing Same Scales	Overlap PCON → Intention
Studying PCON → PCON	Total = 3 Kayhan & Davis, 2016; Li, 2014; Xu, Dinev et al., 2011	Total = 3 Kayhan & Davis, 2016; Li, 2014; Xu, Dinev et al., 2011	Total = 1 Li, 2014
Studying PCON → intention	Total = 19 Bansal et al., 2010; Bansal et al., 2016; Choi & Land, 2016; Dinev et al., 2008; Dinev & Hart, 2006; Gu et al., 2017; Ku et al., 2013; Li, 2014; Li et al., 2011; Li et al., 2017; Li & Unger, 2012; Mao & Zhang, 2013; Min & Kim, 2015; Osatuyi, 2015; Ozdemir et al., 2017; Son & Kim, 2008; Xu, 2010; Xu & Gupta, 2009; Zhang et al., 2018	Total = 7 Dinev & Hart, 2006; Li, 2014; Li et al., 2011; Li et al., 2017; Min & Kim, 2015; Ozdemir et al., 2017; Son & Kim, 2008	
Utilizing same scales	Total = 9 Dinev & Hart, 2006; Kayhan & Davis, 2016; Li, 2014; Li et al., 2011; Li et al., 2017; Min & Kim, 2015; Ozdemir et al., 2017; Son & Kim, 2008; Xu, Dinev et al., 2011		

The two research methods most utilized in the construct-aligned studies were experiment and survey. No study using the experimental approach fell into more than one area of alignment from Table 6. However, only one study fell into all three of the alignment areas for employing surveys (Li, 2014), and two fell into more than one alignment area (Li, 2014; Xu, Dinev et al., 2011).

Seven of the aligned reference studies from Table 6 employed an experimental methodology. Of the three studies investigating the influence of dispositional privacy concerns and site/situation-specific privacy concerns, one study utilized an experimental methodology (Kayhan & Davis, 2016). Of the 19 studies investigating the influence of privacy concerns on intention, six studies utilized an experimental methodology (Bansal et al., 2016; Choi & Land, 2016; Gu et al., 2017; Li et al., 2011; Li & Unger, 2012; Xu, 2010). Of the nine studies utilizing the same scales, two studies utilized an experimental methodology (Kayhan & Davis, 2016; Li et al., 2011).

Thirteen of the aligned reference studies employed a survey methodology. Of the three studies investigating the influence of dispositional privacy concerns and site/situation-specific privacy concerns, two studies utilized a survey methodology (Kayhan & Davis, 2016; Li, 2014). Of the 19 studies investigating the influence of privacy concern on intention, 12 studies utilized a survey methodology (Bansal et al., 2010; Dinev et al., 2008; Dinev & Hart, 2006; Ku et al., 2013; Li, 2014; Mao & Zhang, 2014; Min & Kim, 2015; Osatuyi, 2015; Ozdemir et al., 2017; Son & Kim, 2008; Xu & Gupta, 2009; Zhang et al., 2018). Of the nine studies utilizing the same scales, six utilized a survey methodology (Dinev & Hart, 2006; Li, 2014; Min & Kim, 2015; Ozdemir et al., 2017; Son & Kim, 2008; Xu, Dinev et al., 2011).

Survey methodology emerged as the most appropriate methodology for this research. Surveying was common across all of the aligned studies and the most commonly used across all reference studies (22 out of 31). Chapter 3 referenced studies that demonstrated standard reliability (composite reliability [CR], average variance extracted [AVE]), validity (CR, AVE, square root of AVE), and bias (common method bias [CMB], Harman's single-factor). All constructs under review exhibited consistency of results.

Similar Study Measurements

Numerous studies assessed the same constructs in a manner similar to the proposed study. Several studies examined the influence of DTVP on privacy concerns, utilizing the same scales. Kayhan and Davis (2016) found that dispositional privacy concerns to be positively related to situational privacy concerns. Similarly, Li (2014) found a disposition to privacy as having a positive impact on site-specific privacy concerns. Xu, Dinev et al. (2011) found that DTVP positively affected privacy concerns.

Multiple studies also examined the influence of DTVP on behavioral intention, utilizing the same scales. Li et al. (2017) found that general privacy concern negatively affects behavioral intention (i.e., disclosing personal information). Li et al. (2011) found that general privacy concern negatively affects behavioral intention (i.e., disclose personal information).

Several studies examined the influence of privacy concerns on behavioral intention, utilizing the same scales. Dinev and Hart (2006) found that a higher user Internet Privacy Concern is related to a lower behavioral intention (i.e., provide personal information). Min and Kim (2015) found that perceived privacy concern negatively affects behavioral intention (i.e., giving personal information). Ozdemir et al. (2017) found that the higher a user's privacy concerns, the less likely they are to disclose information. Son and Kim (2008) found that information privacy concerns positively affect public and private action (e.g., complaining, word-of-mouth).

Summary

The chapter provided a discussion of the constructs and theories associated with research in privacy concerns and behaviors. The author provided detailed discussions regarding the inclusion of privacy concerns (unidimensional) and behavioral intentions in the study. Also included were the rationales for excluding other constructs (multidimensional privacy concern, other types of behavior, and other privacy-related variables), as well as relevant theories associated with privacy concerns. The strengths associated with existing studies were discussed, highlighting their consistency of results. The weaknesses and gaps associated with existing research noted a lack of coverage of situational influences on privacy concerns and real privacy-centric situations. The author outlined common methodologies utilized in the literature and standard methods to evaluate reliability, validity, and bias. Finally, the chapter concluded with a review of similar measurements used in the literature.

Chapter 3

Methodology

This study proposed to validate the influence of privacy concerns on behavior intention in an actual privacy-centric situation. Creswell and Plano Clark (2018) provided a template style introduction for mixed method approaches, modeled for research design. An explanatory sequential mixed methods design with interview follow-up was employed. The sequence involved collecting quantitative data first and then contextualizing the quantitative results with qualitative data. The methodology sought to assess if general and situational privacy concerns influenced behavior in an actual situation and provide context for the findings. The first quantitative phase of the study involved collecting questionnaire data from situation-affected LinkedIn users via the Internet to assess whether DTVP influenced situational privacy concerns and influenced behavior intention. The second, qualitative phase, served as a follow-up to the quantitative phase to group the various potential outcomes (derived from variable combinations) and ascertain any context to assist in understanding the outcomes. The explanatory follow-up goal was to provide context to hypothesis support, grounded in variable support degree combinations.

Phase 1 (P1): Quantitative Methodology

This section provides an overview of the quantitative methodology phase of the research. Employing survey methodology began with questionnaire development and its associated constructs, measurement items, and specific validity and reliability measurements. The section continues with a population description and data collection. The section concludes with a discussion of the use of PLS in the analysis.

Twenty-nine of the 31 reference studies with at least one hypothesis related to privacy concerns used survey methodology. All 21 of the scales-aligned studies identified in Table 4 utilized a survey methodology. The author sent the questionnaire to his 1st-degree connections using the LinkedIn Message function and to each of his 2nd-degree connections using the Connect (with a note) function. Appendix B contains a copy of the instrument.

P1: Instrument Development

Using items adapted from validated scales in existing literature, as described in Tables A3, A4, and A5, the researcher operationalized the variables with questions re-worded to fit the research context. The three constructs were measured with a seven-point scale ranging from 1 to 7, anchored with "strongly disagree" and "strongly agree." A single item measured each of the demographic factors (control variables), age and sex. Finally, given participants' ability to modify their LinkedIn profile before contact, the author added a binary scale question as a participant disqualifier.

The researcher used three items adapted originally from Malhotra et al. (2004) and subsequently used in a variety of studies (Kayhan & Davis, 2016; Li, 2014; Li et al., 2014; Li et al., 2017; Li et al., 2011; Xu, Dinev et al., 2011) to measure Disposition to Value Privacy (DTVP). Table A3 reports the results.

As illustrated in Table A4, the author used four items adapted originally from Dinev and Hart (2006) and subsequently re-employed in numerous other studies (Choi & Land, 2016; Min & Kim, 2015; Ozdemir et al., 2017; Son & Kim, 2008; Xu, Dinev et al., 2011) to measure Situation-Specific Internet Privacy Concerns.

The author measured behavioral intention using three items adapted from Molhatra et al. (2004) that were subsequently used to measure behavioral intention in a variety of additional studies on which the research framework was directly based (Li et al., 2011; Min & Kim, 2015) or to evaluate the impact of privacy concerns on intention (Bansal et al., 2010, 2016; Zhang et al., 2018). See Table A5.

P1: Sample and Data Collection

A preliminary methodology to determine the viability of the convenience population yielded positive results. The first step was to search all of the author's LinkedIn connections using the search term "SIGINT" (signals intelligence, a generic term used for demonstration by ICWATCH developers) (re:publica, 2015), which resulted in 3,392 1st- and 2nd-degree connections; however, only 1,316 were readily accessed (due to server-side search limitations of 1000 non-unique results at a time). The second step was to reduce this list to individuals who were both (a) a LinkedIn connection and (b) listed on ICWATCH, which resulted in a reduction to 496 connections (~37%). It was assumed that this reduction would remain consistent across all the author's 1st- and 2nd-degree connections and was anticipated to yield a sample population for this study of ~1,275 individuals. However, this was merely an initial support metric and was not intended to account for additions resulting from new LinkedIn connections.

Two additional enhancements overcame the server-side search limitations mentioned earlier, search filters (e.g., industry, location, etc.) and premium membership. The search process was repeated through multiple iterations to identify a final population of 1,310 individuals both on LinkedIn and ICWATCH. Based on a separate study by Claybaugh and Haseman (2015), which resulted in a 19% response rate, 260 participants were expected to participate. This was considered viable as a total number of participants from a cross-section of reference studies had the following characteristics: largest = 889, smallest = 100, median = 285, mode = ~341.

The survey was administered to the 1,310 individuals thru LinkedIn directly. Due to a LinkedIn message size restriction, a 300-character message was created to invite each participant. The message read, “"Please participate in my Ph.D. dissertation study, investigating linkages between privacy and behavior of users like you, who had their LinkedIn account scraped and made searchable through ICWATCH, a third-party website. The anonymous survey is available at https://www.surveymonkey.com/r/CP5JWGS"

For 1st-degree connections, the invite was sent using the "Send a message" function. For 2nd-degree connections, the invite was sent using the "Connect with note" function. While the 300-character limit only applied to the 2nd-degree connection invites, the same invite was used for both degrees of connection to maintain consistency.

Initially, it was observed that while 2nd-degree connections were accepting the connection request, there was not a visible correlation with a subsequent survey response. Therefore, it was assumed that invitees merely accepted the connection request and did not see the invite. To mitigate this, each time a 2nd-degree connection accepted the request to connect, a short one-time follow-up message was sent using the now available "Send a message" feature (as they were now 1st-degree connections). The follow-up message read, "Thank you for accepting my connection request. If you haven't already, I hope you will consider participating in my Ph.D. dissertation survey, which is anonymous."

From the 1,310 invites sent via LinkedIn, there were 78 responses; 13 were not used, as eight were incomplete and five indicated they were not sharing their profile publicly (disqualification), resulting in 65 valid responses (4.96%). Participant demographics are described in Table 5.

Table 5

Demographic Information of the Questionnaire Respondents

Demographic Variables	**Category**	**Frequency (%)**
Sex	Female	8 (12.31%)
	Male	57 (87.69%)
Age	< 20	0 (0%)
	20-29	1 (1.54%)
	30-39	9 (13.85%)
	40-49	16 (24.62%)
	50+	39 (60.00%)

An ad-hoc post-invite analysis using the Social Security: Get Ready For Baby website (https://www.ssa.gov/OACT/babynames/index.html) was used to derive approximate sex demographics of the population, resulting in a 1067 male (81.45%) to 149 female (11.31) distribution, with 94 indeterminate.

Phase 2 (P2): Qualitative Methodology

As part of the mixed method approach, the author invited select participants to participate in a one-on-one interview (i.e., follow-up) to contextualize the quantitative findings. Several reference studies also utilized interviews as part of a mixed methods approach, either to create an instrument (Cichy et al., 2014; Ku et al., 2013; Malhotra et al., 2004; Smith et al., 1996; Treiblmaier & Chong, 2011) or to contextualize results (Ball et al., 2012). This study employed a purposeful sampling approach, utilizing a simple scoring model to identify and invite a minimum of three participants from pre-defined variable outcome groups. What follows is a discussion of the qualitative portion of the study, specifically, how the population was identified and invited for follow-up. Next, a discussion regarding the demographics of the interview population and the participants is described. Finally, an elaboration on the methodology used to derive the qualitative data for analysis is discussed.

P2: Interview Development

As this research was explanatory in design, it employed semi-structured interviews, which modeled the approach used by Ball et al. (2012). Also, to support an explanatory design, the semi-structured approach employed topics aligned directly with the questionnaire. This served to elaborate on the underlying concepts influencing the participant's responses in the questionnaire. The topics also served a dual-purpose as the categories for code alignment; categories were modeled after an approach used by Cichy et al. (2014).

Since the research design assumed that this situation was a breach of privacy, the first topic prompted a discussion on the participant's belief regarding this matter. It was initiated by stating, "For the next few minutes, let's discuss if this is a breach of privacy." The second topic prompted a discussion on the participant's disposition to value privacy and was initiated by stating, "For the next few minutes, let's discuss your disposition to value privacy."

The third topic prompted a discussion regarding the participant's level of privacy concern regarding the situation related to the ingestion of their LinkedIn information into ICWATCH. It was initiated by stating, "For the next few minutes, let's discuss your level of concern regarding LinkedIn scraping/posting your data." The fourth topic prompted a discussion on the participant's intention to modify their LinkedIn profile's visibility and was initiated by stating, "Finally, let's discuss your intention to modify your LinkedIn profile's visibility." At the end of each interview, the participant was given the opportunity to provide any additional thoughts by stating, "Are there any other additional thoughts or comments you might have?"

P2: Sample and Data Collection

Only a subset of Phase 1 participants comprised the convenience population for this phase of the study, expressly, those who (a) completed the questionnaire associated with Phase 1 (quantitative), and (b) indicated a willingness to be interviewed (per questionnaire response). A simple scoring model was selected to derive each variable's least ambiguous representation for respondent assignment to an outcome group. The scoring model calculated the numerical sum of results for each variable's questions, then selected the top and bottom 25% of all scores within each variable to derive the least ambiguous strong and weak representations of the variable, as shown in Table 6.

Table 6

Internal Consistency and Discriminate Validity of Constructs

Constructs	# of Questions (7-pt Likert)	+ or -	Score Range	Top 25%	Bottom 25%
BITN	3	neg	0-21	<13	>17
DTVP	3	pos	0-21	>18	<15
SIPC	4	posx	0-28	>21	<16

Note. H = high score, L = low score

Respondents were assigned to one of the eight possible outcome groups based on score calculations, as shown in Table 7. Of the 65 respondents, only 11 volunteers had appropriate scores for assignment to five outcome groups (OG-A, OG-B, OG-E, OG-G, and OG-H). However, any respondents groups not meeting a 5% population representation were not invited for interviews, as they were considered outliers.

Table 7

Outcome-group Score Results and Distribution

Outcome-Group	BITN	DTVP	SIPC	Qualified	Volunteer
OG-A	>17	<15	<16	7	5
OG-B	<13	<15	<16	1	1
OG-C	>17	<15	>21	0	0
OG-D	<13	<15	>21	0	0
OG-E	>17	>18	<16	1	1
OG-F	<13	>18	<16	0	0
OG-G	>17	>18	>21	1	1
OG-H	<13	>18	>21	4	3

As mentioned earlier, the interview methodology modeled the approach utilized by (Ball et al., 2012), employing semi-structured interviews around four topics; however, the interviews were remote rather than face-to-face. An email was sent to the volunteers in groups A and H to solicit a date/time for the follow-up interview, with a total of six participants responding, a 50/50 split between groups as shown in Table 8. Once a date/time was confirmed, a web conference invite was emailed to the participant, and interviews were conducted via web conferencing (Zoom). During each, the author confirmed the participant ID, provided a brief description of the interview purpose and process, then provided each topic sequentially (as discussed earlier). A transcription of each of the interviews is provided in Appendix E. Each participant was also provided an opportunity to convey additional comments at the end of the interview, modeled as a fifth topic.

Table 8

Individual Participant Score Results and Distribution

Participant	Outcome-Group	BITN	DTVP	SIPC
11269613365	OG-A	21	3	4
11223476508	OG-A	21	6	5
11188138618	OG-A	18	6	8
11251351842	OG-H	9	21	28
11224014306	OG-H	12	21	28
11205114603	OG-H	9	21	25

The six-person sample demographic was all male and all in the 50+ age category, as depicted in Table 9.

Table 9

Demographic Information of Interview Participants

Demographic Variables	Category	Frequency (%)
Sex	Female	0 (0%)
	Male	6 (13.33%)
Age	< 20	0 (0%)
	20-29	0 (0%)
	30-39	0 (0%)
	40-49	0 (0%)
	50+	6 (100%)

A methodology provided by Creswell and Plano Clark (2018) was employed to support generating and utilizing the qualitative data. In the first part of the methodology, which is relevant to this section, the data must be prepared for analysis (i.e., transcribed and formatted), explored (read and understood), then coded and analyzed (e.g., interrelate categories). In the second part of the methodology, which is covered later, the data is analyzed and represented (Appendices A and D), the results summarized and related (Table 14), and the data and results validated.

Data Preparation. Interviews were recorded and then transcribed using a two-step process. The audio recording was done using the Zoom cloud recording feature, which resulted in a downloadable Moving Picture Experts Group (MPEG-4) file of the interview. Transcription was accomplished using a cloud-based tool called Otter, which performed the speech-to-text translation. The first step was to upload the MPEG-4 file into Otter, which resulted in a rough draft transcription of the recording. The second step leveraged the cloud-based Otter.ai editing tools with synchronized playback (e.g., the service would highlight words synchronized to the audio). A second recording and transcription methodology was in place for redundancy using the TapeACall application; however, this was for backup only, and the additional files were not utilized.

Data Exploration. Each of the interviews was read multiple times to explore the data. In this context, data exploration was limited to understanding the completeness and context of a particular snippet and annotating each onto a separate card. This exploration yielded 163 snippets, of which 149 were carried forward into step three. During exploration, it became evident that the interview statements reflected the multi-dimensional aspects of privacy concern and other constructs well-represented in existing privacy literature.

Coding and Analysis. Using a category/code approach, the snippets were separated into codes and then grouped by category. After analyzing each of the 149 snippets, 12 codes were derived. As noted earlier, the codes were operationalized using constructs adapted from existing literature, as described in Table A6. A code/snippet alignment validation was also conducted, which is discussed in a later section, resulting in 139 usable code/snippet alignments, as shown in Appendix D.

Summary

This chapter provided a detailed discussion of the mixed method approach used in the research. The first half elaborated on the quantitative portion. This portion employed a survey methodology, using instrument scales operationalized from existing literature. LinkedIn connections, numbering 1,310, were sent an invite, with a valid response rate of 4.96%, skewed heavily towards males over 50 years of age. Next, the qualitative portion of the methodology was described. Participants were divided into variable-aligned outcome groups, based on the quantitative findings, using a simple scoring model. Only two of the groups met the 5% representation threshold, of which only six participants were interviewed. Finally, the multi-step methodology used to transform interview data into category/code aligned data for analysis.

Chapter 4

Results

In this chapter, the results of the data analysis are reported in various discussions and tables for both the research's quantitative and qualitative phases. The quantitative portion describes demographic statistics, findings from validity and reliability testing, and hypothesis analysis. The qualitative phase of the research also includes demographic statistics and validity and reliability support, integrated with the quantitative data for contextual support. Finally, the chapter culminates in a summary of the results.

Phase 1 (P1): Quantitative Data Results

This section provides a discussion of the quantitative findings. The section elaborates on the validity, reliability, and consistency of findings from the measurement model. This is followed by a discussion of the data analysis methodology. Finally, the section concludes with an elaboration of the results of the quantitative analysis.

P1: Measurement Model Findings

The validation methodology used SmartPLS analysis for convergent validity, the degree to which the same construct measures are related or agree. Xu, Luo et al. (2011) note, "In PLS, we conducted three tests to determine the convergent validity of measured, reflective constructs in a single instrument: reliability of items, composite reliability of constructs, and average variance extracted (AVE) by constructs" (p. 47). Reliability of items was assessed in several scales-aligned studies (Dinev & Hart, 2006; Kayhan & Davis, 2016; Li et al., 2011; Li et al., 2017; Son & Kim, 2008; Xu, Dinev et al., 2011). This study assessed each item's factor loading to ensure it exceeded a minimum threshold of 0.70 (Bollen, 1989). All exceeded the threshold, as shown in Table 10.

Table 10

Loading and Cross-Loadings of Measures

Constructs		BITN	DTVP	SIPC
BITN				
	BITN1	0.826	-0.351	-0.436
	BITN2	0.880	-0.331	-0.462
	BITN3	1.041	-0.417	-0.543
DTVP				
	SPCN1	-0.346	0.859	0.651
	SPCN2	-0.412	0.943	0.680
	SPCN4	-0.418	0.769	0.568
SIPC				
	SIPC1	-0.418	0.748	0.952
	SIPC2	-0.480	0.653	0.905
	SIPC3	-0.510	0.640	0.899
	SIPC4	-0.476	0.592	0.818

Composite reliability of constructs was also assessed in two scales-aligned studies (Kayhan & Davis, 2016; Xu, Dinev et al., 2011). This study also assessed that each construct's composite reliability exceeded the minimal criterion of 0.70 (Nunnally, 1978), which all of them achieved, as shown in Table 11.

Table 11

Internal Consistency and Discriminate Validity of Constructs

Constructs	Composite Reliability (CR)	Average Variance Extracted (AVE)	Correlations		
			DTVP	SIPC	BITN
BITN	0.942	0.846	0.920		
DTVP	0.894	0.739	-0.400	0.860	
SIPC	0.941	0.800	-0.525	0.738	0.895

Note. Square root of AVE on the diagonals, correlations on off-diagonals

AVE was assessed in several scales-aligned studies (Dinev & Hart, 2006; Kayhan & Davis, 2016; Li, 2014; Min & Kim, 2015; Xu, Dinev et al., 2011). This study measured the AVE to ensure it exceeded the minimum level of 0.50 (Fornell & Larcker, 1981), which all did, as shown in Table 11.

Discriminant validity is the degree to which different constructs are unrelated. Throughout the reference studies, discriminant validity was assessed using the square root of AVE and factor loadings/cross-loadings. The square root of the AVE was assessed in several of the scales-aligned studies (Li et al., 2011; Li et al., 2017; Min & Kim, 2015; Ozdemir et al., 2017; Son & Kim, 2008; Xu, Dinev et al., 2011). This study found that it was greater than the correlation between that construct and any other constructs (Fornell & Larcker, 1981), which it was, as shown in Table 11. Factor loadings and cross-loadings were also assessed in several scales-aligned studies (Li, 2014; Li et al., 2017; Ozdemir et al., 2017; Xu, Dinev et al., 2011). This study assessed that items were loaded more strongly on their intended construct than others (Gefen & Straub, 2005), as shown in Table 10.

Reliability refers to the internal consistency of items. Specifically, responses are consistent across items and participants, assessed using CR and AVE. CR was assessed in several scales-aligned studies (Dinev & Hart, 2006; Li et al., 2011; Li et al., 2017; Min & Kim, 2015; Ozdemir et al., 2017; Son & Kim, 2008). This study exceeded 0.70 (Bagozzi & Yi, 1988; Fornell & Larcker, 1981) as shown in Table 11. AVE was assessed in several scales-aligned studies (Dinev & Hart, 2006; Li, 2014; Li et al., 2011; Li et al., 2017; Ozdemir et al., 2017). This study exceeded 0.5 for all items (Bagozzi & Yi, 1988; Fornell & Larcker, 1981), as shown in Table 11.

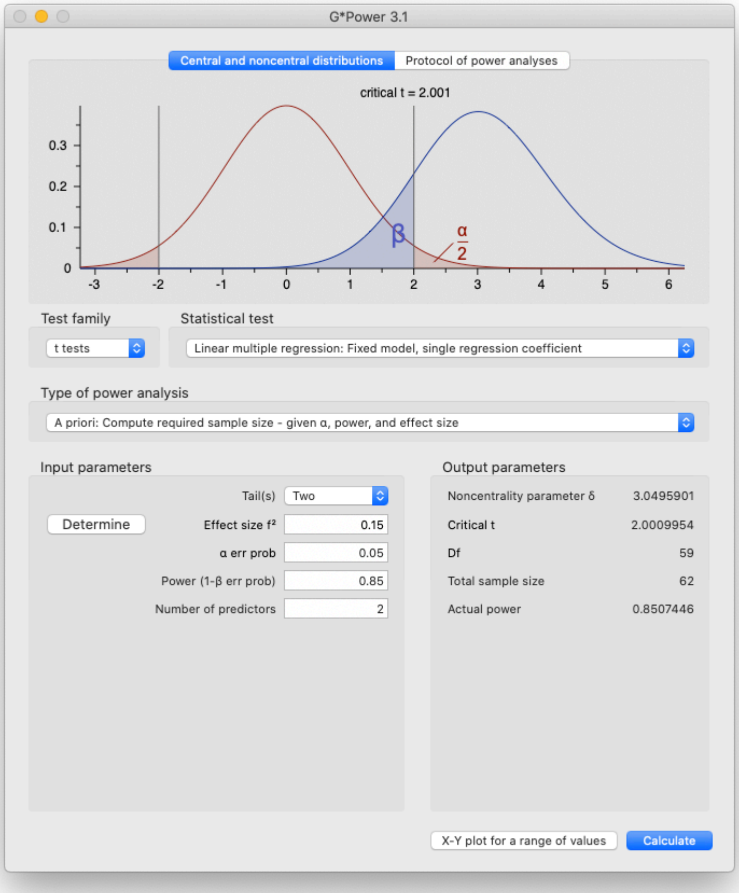
P1: Data Analysis, Partial Least Squares (PLS)

To measure the (a) influence of DTVP on situation-specific Internet privacy concerns and (b) situation-specific Internet privacy concerns on a user's intention to engage in privacy-protecting behaviors (modify their profile settings or keywords), the quantitative analysis utilized Partial Least Squares (PLS). Of the three studies investigating the influence of dispositional privacy concerns and site/situation-specific privacy concerns, all three utilized PLS. Of the 19 studies investigating the influence of privacy concern on intention 11 utilized PLS (Gu et al., 2017; Ku et al., 2013; Li, 2014; Li et al., 2011; Li et al., 2017; Li & Unger, 2012; Mao & Zhang, 2013; Osatuyi, 2015; Ozdemir et al., 2017; Xu, 2010; Xu & Gupta, 2009). Of the nine studies utilizing the same scales, six utilized PLS (Kayhan & Davis, 2016; Li, 2014; Li et al., 2011; Li et al., 2017; Ozdemir et al., 2017; Xu, Dinev et al., 2011). However, while only one study fell into all three of the alignment areas for using PLS (Li, 2014), two fell into more than one alignment area (Li, 2014; Mao & Zhang, 2013). The usage of PLS in a quantitative approach, especially survey methodology, is well represented in the literature. Thirty-one of the reference studies had at least one hypothesis related to privacy concern, of which 16 used PLS. Thirteen of the 21 aligned reference studies utilized PLS.

Initially, it was assumed that a sample size of 65 would be adequate, since, as noted by Li et al. (2011), "PLS requires a much smaller sample size than other structural equation modeling (SEM) techniques" (p. 439). However, to validate this a software solution called G*Power 3.1 was used to calculate the number of participants needed for PLS analysis, which indicated a minimal sample size of 62 was needed, as shown in Figure 2.

Figure 2

*G*Power Results*


G*Power 3.1
Central and noncentral distributions
Protocol of power analyses
critical t = 2.001
0.3
0.2
0.1
0
-3
-2
-1
0
1
2
3
4
5
6
β
α
2
Determine
X-Y plot for a range of values
Calculate

Test family: t tests

Statistical test: Linear multiple regression: Fixed model, single regression coefficient

Type of power analysis: A priori: Compute required sample size - given α, power, and effect size

Input parameters

Tail(s)	Two
Effect size f²	0.15
α err prob	0.05
Power (1-β err prob)	0.85
Number of predictors	2

Output parameters

Noncentrality parameter δ	3.0495901
Critical t	2.0009954
Df	59
Total sample size	62
Actual power	0.8507446

Before the analysis, the data were normalized for ingestion into the software. Specifically, fields were renamed to match the construct names and break out categorical control variables (age and sex) into dummy variables to incorporate into the model and were ingested with no errors. The analysis utilized the SmartPLS software application, and analysis was conducted using both the Consistent PLS Algorithm (PLSc) and Consistent PLS Bootstrapping as the model uses reflective factors. Specific settings for each analysis are provided in Table 12.

Table 12

SmartPLS Configurations

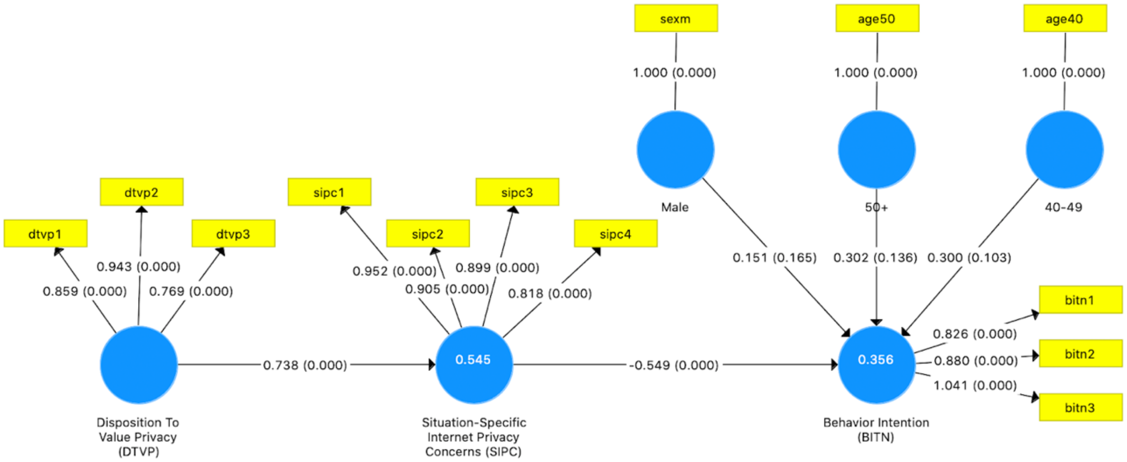
SmartPLS Setting	**Bootstrap**	**PLSc**
Initial Calculations	Connect all LV's for Initial Calculation	Connect all LV's for Initial Calculation
Weighting Scheme	Path	Path
Maximum Iterations	1000	1000
Stop Criterion	7	7
Subsamples	5000	
Amount of results	Complete Bootstrapping	
Confidence Interval Method	Bias-corrected and accelerated (BCa) Bootstrap	
Test Type	Two-Tailed	
Significance Level	0.05	

P1: Structural Model Findings

Path coefficients and path significance for the two hypotheses are shown in Figure 3 and summarized in Table 13.

Figure 3

Research Model with Results and Significance



Note. As each of these control variables was categorical, each category was modeled as dummy (binary) variables; age used five dummy variables, and sex used two. Four dummy variables (30-39, 20-29, <20, and female) had insufficient analysis samples.

Table 13

Hypothesis Testing Results

Hypothesis	Path Coefficients	t value	p-value	Supported?
H1	0.738	8.802	< 0.001	y
H2	-0.549	5.353	< 0.001	y
Age → BITN (50+)	0.302	1.492	0.136	
Age → BITN (40-49)	0.300	1.631	0.103	
Sex → BITN (Male)	0.151	1.389	0.165	

Hypothesis One (H1) predicted that as a person's disposition to value privacy increased, their situation-specific Internet privacy concerns would also increase. The effect of DTVP on SIPC was shown to be both positive and significant (B=0.738, p<0.001), therefore supporting H1. Hypothesis Two (H2) predicted that as a person's situation-specific Internet privacy concerns increased, their willingness to continue sharing information publicly on LinkedIn would decrease. The effect of SIPC on BITN was negative and significant (B=-0.549, *p*<0.001), therefore supporting H2.

Path coefficients and path significance for the control variables are also illustrated in Figure 3. The control variables of age and sex were analyzed for their effect on BITN, and neither affected BITN significantly. Only two age groups were modeled 50+ (B=0.302, *p*=0.136) and 40-49 (B=0.300, *p*=0.103); however, there were insufficient samples in the other three age groups (30-39, 20-29, and 19 or less) to analyze. Being male also had no significant effect on BITN (B=0.151, *p*=0.103); again, there was an insufficient number of females to analyze.

Phase 2 (P2): Qualitative Data Results

This section provides a discussion of the qualitative findings. Creswell and Plano Clark (2018) describe the purpose of the integration as connecting the quantitative and qualitative phases. The first part of the section reviews the validity, reliability, and consistency findings from the interview data, followed by a discussion of the sequential integration methodology. Finally, the section concludes with an elaboration of the qualitative analysis results, including the integrated results.

P2: Measurement Model Findings

Creswell and Plano Clark (2018) note, "In general, reliability plays a minor role in qualitative research because the inquirer instead emphasizes the value of his or subjective interpretations" (p. 217). Thus, validation focused on two primary goals, transcription accuracy and coding alignment. A validator was recruited to independently utilize the

Otter.ai tool to ensure that transcriptions were accurate. The validator reviewed each transcription within the tool and agreed with transcriptions.

In addition, two rounds of code-snippet validation were also conducted. First, six reviewers validated the code/snippet alignment by dividing it into three groups of two each. Each pair was aligned with both a code definition and an example snippet that best represented that code. The code-snippet pairs were distributed across the groups such that each code would receive two reviews. A simple scoring model was implemented for the review, asking each member to rate their concurrence with the author's alignment and provided example, broken out as "Agree = 1". "Good as anything = .5", or "Something else = 0". For "Something else," the reviewer was asked to suggest a different code. Of the six participants, only four completed the peer reviews: one from both groups one and three and two from group two; one of the reviewers from group two reviewed every item, thus providing three total reviews. The minimum concurrence score was set for two, and 142/149 (95.90%) codes met or exceeded this score, as shown in Table D1. The seven snippets that did not meet the minimum score were dropped.

Second, the author created a unique ID for each snippet/code pair and tagged the appropriate text within each interview transcript, ensuring each snippet/code pair was unique. This review identified seven snippets that required de-confliction due to overlap. Post review, four of the seven codes were separated, and for the remaining three, one of the conflicting codes for each was dropped. After all the validation was completed, 139 snippet/code pairs remained for analysis.

P2: Data Analysis, Sequential Integration

A sequential integration process was used to integrate the findings from both phases of the research. The integration's primary focus was to map shared category-code findings from each outcome group to the hypotheses. A final consolidated mapping provided a richer, more contextual understanding of the quantitative findings via a joint display, as shown in Table 14. Creswell and Plano Clark (2018) note,

> Researchers also need to represent the connection between the initial quantitative results and the following-up qualitative results with a joint display or graph. The purpose of such a results display is to make specific the link between the two connected databases and to help visualize how the qualitative findings enhance the understanding of the quantitative results (p 237).

For each of the five categories, standardized methodology generated the contextual findings. First, code/snippet pairs were broken out by the two outcome groups. Next, the total number of snippets for each code/group pair was quantified, and the number of participants providing the associated snippets. Then, representative snippets were selected based on score in that the highest score of three was selected when possible. If multiple snippets were equal in score, best judgment was used based on the current context. Subsequently, an analysis was conducted to validate if the snippets and participants were normally distributed, then record the observations and outliers associated with each.

The hypothesis support analysis utilized the same methodology, with some additional steps in the beginning. First, category/code pairs were provided with their associated hypothesis. Categories for DTVP and SIPC were associated with Hypothesis One (H1).

Categories for SIPC and BITN were associated with Hypothesis Two (H2). Next, only codes that were shared between the category pairs were selected for analysis. Finally, representative snippets were selected for each code-group to provide context, distributions analyzed, outliers identified, and observations were noted.

The analysis methodology was applied in three passes through the code/snippet pairings. First, an analysis was conducted on all codes and categories (including supplementary). Second, an analysis was conducted on code/snippet pairs for each category individually (including supplementary). Finally, an analysis was conducted on categories aligned with the hypotheses, and findings were integrated with the quantitative results.

P2: Code Analysis Findings

All qualitative findings are presented in detail in Appendix D. Table D1 details all code-snippet pairs' findings derived from the interviews. The analysis resulted in 139 snippets associated with 12 unique codes across two outcome groups (A and H) in a 43.17(A)/56.83%(H) breakout. Calculations using all 12 codes and all five categories resulted in a distribution that did not differ significantly from the norm, as shown in Table A7. The following describes the specific findings by both group-participants and group-snippet.

Group-Participant: All Codes. There were six participants, all of whom were male and 50 or older, divided equally into the two outcome groups. Calculations using all 12 codes and six participants resulted in a distribution that did not differ significantly from the norm, as shown in Table A7; however, Group H contributed 31.67% more snippets.

Only two codes were discussed by all six participants, while various combinations of five participants discussed another four. All participants recognized the advantages of having a LinkedIn profile (benefit) and knowledge of internet collection and analysis activities (collection). However, only five indicated their intention (or lack thereof) to make changes to their profile (behavior) or their inclination to value privacy (GPCN), both of which were directly reflective of the underlying constructs. Five participants also discussed their expectations of privacy on sites (PRBF) or how their data was being used (usage).

Unlike their counterparts, Group A participants were more deliberate in their contentions. They did not have any codes represented by only one participant; they had five codes with zero snippets. However, only single participants from Group H indicated contributions by their decision on what/when to share (control), accuracy or inaccuracy of the posted data (errors), and/or personality traits. Group H was more deliberate in the overall number of items all members acknowledged, with a total of six (behavior, benefit, collection, GPCN, SPCN, and usage), as opposed to their group A counterparts at only four (benefit, collection, control, PRBF). As expected, with group H the least ambiguous representation of each variable, they were the only group to present all 12 codes; however, with only one participant in three codes (control, errors, PNTR). Group H was also the only group to indicate the influence of negative experiences (invasion), personality quirks (PNTR), laws (regulations), and concerns with this situation (SPCN).

Participants in group A did not present any notions regarding the influence of inaccuracies (errors), previous negative experiences (invasion), personality quirks

(PNTR), laws, regulations, or policies, or the situation (SPCN). Only single participants from group H indicated the influence of either errors or personality traits.

Group-Snippet: All Codes. There were 139 snippets separated into the two outcome groups in a 43.17/56.83% breakout, respectively. Calculations using all 12 codes and associated snippets resulted in a distribution that did not differ significantly from the norm, as shown in Table A7; however, group H participants contributed 64.71% more frequently.

There was a 50/50 split on the group presenting the most snippets for each of the four codes having more than the average (11.58) number of snippets. Group A provided the most snippets for the two codes having the most, 80.00% of the 25 snippets for PRBF and 90.01% of the 22 snippets for control. However, group H provided the most snippets for the second two codes having the most snippets, 76.47% of the 17 snippets for usage and 66.671% of the 12 snippets for collection.

Group A did not make any contributions for five codes (errors, invasion, PNTR, regulations, and SPCN), which would indicate that these were not a factor in the lesser degree representations of the variables. Group H indicated that both control and PNTR were underlying factors; however, two snippets only supported each.

Category 1: Breach of Privacy. The first interview topic sought to determine if the situation was a breach of privacy by stating, "For the next few minutes, let's discuss if this is a breach of privacy." The research design incorporated this topic to validate the assumption of whether the participants considered this situation a breach of privacy. Table A8 details the findings for this category derived from the interviews. Specifically, 10 codes were supported by 29 snippets provided by all six participants across the outcome groups in a 37.93(A)/62.07%(H) breakout, with neither group presenting either errors or PNTR. Separate calculations using all 12 codes, with all six participants and associated snippets, resulted in disparate distributions; the code-participant distribution did differ from normal, while the code-snippet distribution did not, as shown in Table A7.

Across both groups, 66.67% did not believe this situation was a breach of privacy, with the remaining indicating they were unsure. Both groups indicated that their inclinations to worry about privacy (GPCN) and potential for a loss of privacy (PRBF) were underlying factors, with group A providing 88.89% of the nine for PRBF; which presented at more than twice the number of snippets of the next most extensive code (invasion) response at four. Group A was also the only group to indicate that their ability to control their data was a factor. Group H had 133.33% more participant engagements at 14 and 63.64% more snippets at 18. Consistent with their higher degree representation of the variables, group H also contributed 63.64% more snippets and seven unique codes (behavior, benefit, collection, invasion, regulation, SPCN, and usage). As stated earlier, invasion had the second most snippets, indicating that previous negative experiences were a factor for group H.

While both groups indicated that their inclination toward privacy was a factor, it was unsubstantial, with only a single participant from each group presenting a single snippet. Participants in group H indicated that maintaining their profile (behavior) and potential legalities and liabilities (regulation) were factors, again minimal as a single participant only presented each with a single snippet. Unlike the others in group H, one of the participants affirmed that this situation was not a privacy breach.

Category 2: DTVP. The second interview topic sought to elicit the participant's disposition to value privacy by stating, "For the next few minutes, let's discuss your disposition to value privacy." Table A9 details the findings for the DTVP category derived from the interviews. There were 11 codes supported by 34 snippets provided by all six participants across the outcome groups in a 35.29(A)/64.71%(H) breakout; however, the code for behavior was not presented by any participant. Separate calculations using all 12 codes, with all six participants and associated snippets, resulted in distributions that did not differ significantly from the norm, as shown in Table A7.

Both groups discussed elements of control (what to share, how much to share, and when to engage in sharing), with group A providing 77.78% of the nine snippets for control, which presented nearly twice the next most extensive code (GPCN and PRBF) responses at four. Consistent with earlier trends, group H had 166.67% more participant engagements at 16 and 83.34% more snippets at 22. All group H members affirmatively expressed their inclination to value privacy (GPCN).

While both groups indicated that the advantages of having a LinkedIn profile were a factor, it was negligible, with only a single participant from each group presenting a single snippet. Group A did not make any contributions for six codes (collection, errors, invasion, PNTR, regulation, and usage), which would indicate that these were not a factor in the lesser degree representations of the variables. Participants in group H indicated that while collection, errors, invasion, and usage (four codes) were factors, all were minimal as a single participant only presented each with a single snippet.

Category 3: SIPC. The third interview topic sought to derive the participant's level of privacy concern regarding the situation by stating, "For the next few minutes, let's discuss your level of concern regarding LinkedIn scraping/posting your data." Table A9 details the findings for the SIPC category derived from the interviews. There were eight codes supported by 28 snippets provided by all six participants, across the outcome groups in a 39.29(A)/60.71%(H) breakout, with neither group presenting four codes (benefit, GPCN, invasion, and PNTR) in this category. Separate calculations using all 12 codes, with all six participants and associated snippets, resulted in distributions that were not normally distributed, as shown in Table A7.

During the interviews, members of both groups discussed internet collection and analysis activities (collection) and the ambiguity on the ultimate purpose for the scraped data (usage). However, group A provided 33.33% more snippets at three for collection, and group H provided 500.00% more snippets at six for usage. Consistent with the trend, group H had 66.67% more engagements at 10 and 54.55% more snippets at 17. All group H members affirmatively expressed privacy concerns regarding this situation (SPCN) and the potentially nefarious applications of their scraped data (usage).

Group A did not make any contributions for six codes (behavior, benefit, errors, GPCN, PNTR, and regulations), which would indicate that these were negligible factors in the lesser degree representations of the variables. Also, only a single participant from group A presented the only four snippets for control in this category. Group H did not make any contributions for five codes (benefit, control, GPCN, PNTR, and PRBF), which would indicate that these were minor factors in the higher degree representations of the variables.

Category 4: BITN. The fourth interview topic sought to derive the participant's intention to modify their LinkedIn profile's visibility by stating, "Finally, let's discuss your intention to modify your LinkedIn profile's visibility." Table A9 details the findings for the BITN category derived from the interviews. There were nine codes supported by 27 snippets presented from all six participants, across the outcome groups in a 59.25(A)/40.74%(H) breakout, with neither group presenting three codes (PNTR, regulations, and SPCN) by any participant in this category. Separate calculations using all 12 codes, with all six participants and associated snippets, resulted in distributions that were not normally distributed, as shown in Table A7.

The groups diverged in their intention to modify their profiles, although both agreed there were advantages to having a LinkedIn profile (benefit). While benefit presented at 100%, only 83.33% of all participants discussed their intentions to modify their profile (behavior, with only group H affirming this intent), resulting in the most associated snippets in this category. Unlike the previous categories, group A had 11.11% more engagements at 10 and 45.45% more snippets at 16.

Group A did not make any contributions for three codes (collection, errors, and invasion), which would indicate that these were not a factor in the lesser degree representations of the variables. Participants in group A also indicated three codes (control, GPCN, and PRBF) were factors, again irrelevant as a single participant only presented each with a single snippet. Group H did not make any contributions for four codes (control, GPCN, PRBF, and usage), which would indicate that these were unimportant in the higher degree representations of the variables. Participants in group H also indicated three codes (collection, errors, and invasion) were factors, yet irrelevant as a single participant only presented each with a single snippet.

Category 5: Supplementary. The fifth interview topic sought to provide any additional reflections from the interview subjects by stating, "Are there any other additional thoughts or comments you might have?" Table A10 details the findings for the supplementary category derived from the interviews. There were eight codes supported by 21 snippets presented from only five participants across the outcome groups in a 47.62(A)/52.38%(H) breakout, with neither group presenting four codes (behavior, GPCN, PNTR, and SPCN) by any participant in this category. Separate calculations using all 12 codes, with only five participants and associated snippets, resulted in distributions not normally distributed, as shown in Table A7.

Group A was the only group to indicate that their decisions on what/when to share (control) and expectations of privacy on sites (PRBF) were factors by 66.67% of the participants. Group H had 16.67% more participant engagements at 7 and 10.00% more snippets at 11; however, one group A member did not contribute to this category. Group H was the only group to indicate that laws (regulations) and how their data was being used (usage) were factors, by 66.67% of the participants.

While both groups indicated that knowledge of internet collection and analysis activities (collection) was a factor, it was unimportant. Only a single participant from each group presented a single snippet. A single group A participant acknowledged that the advantages of having a LinkedIn profile were a factor with a single snippet. Group A did not make any contributions for four codes (errors, invasion, regulation, and usage), indicating that these were not factors in the lesser degree representations of the variables. As mentioned earlier, one participant in group A did not contribute any snippets. Group H did not make any contributions for three codes (benefit, control, and PRBF), which would indicate that these were negligible factors in the higher degree representations of the variables. Participants in group H also indicated three codes (collection, errors, and invasion) were factors. However, again these were minimal, with a single participant only presenting each with a single snippet.

P2: Sequential Integration Findings

Hypothesis One (H1). The quantitative analysis found significant support for H1, showing that DTVP has a positive effect on SIPC. Table 14 details the findings for the integration of results associated with H1. Overlap analysis of categories DTVP and SIPC resulted in seven codes supported by 40 snippets from all six participants.

Table 14

Sequential Integration Results

Hypo/ Code	OG	Participants	Snippets	Representative Snippets
H1/CNTL	A	3	11	• “So if if I don't want uh, if if I want to be private, that I don't engage, that's that's the only way to be completely private." (11188138618, CNTL02, DTVP) • “Okay. So once again, I mean it's, it's up to me to be careful of what I put out there in terms of uh you know what content I make available." (11269613365, CNTL12, SIPC)
H1/PRBF	A	2	5	• “Um so uh I don't um believe that knowing my name, and uh, and uh knowing my disposition, but through conversation, either over the phone or uh, or in person is anything more than just um that person that I'm engaging with, using their uh, their skills and their uh techniques of a, of a um observation to to make a make a deduction." (11188138618, PRBF20, DTVP) • “So maybe you have a question about it, you know, we've been instructed to contact the government, if you have, if you have any concerns, so uh most of that stuff has been vetted that that I would ever talk about, I have very little out there." (11269613365, PRBF15, SIPC)

(continued)

Hypo/ Code	OG	Participants	Snippets	Representative Snippets
H1/COLL	H	1	3	• “I, I suspect the bigger the bigger issue and bigger concern um would be to take uh the information from the OPM or some of the other databases that have been breached and and kind of uh meld them together if you will." (11251351842, COLL09, DTVP) • “So uh I think I need some questions answered, um before I can move forward in having worked in the IC community for a short period of time, just a couple years, I know the capabilities of what they can do and and uh things they can look at." (11224014306, COLL05, SIPC)
H1/ERRS	H	1	2	• “Professional reasons I had to and uh but every now and then I go back in there and I make some adjustments, make some updates, take some stuff off that are no longer relevant." (11205114603, ERRS01, DTVP) • “But uh, but for me, I have no need to be in that um in that world anymore. Uh, so as time goes on I, I remove a lot of those specific key terminologies simply because um that's in the past and it's no longer relevant." (11205114603, ERRS03, SIPC)
H1/REGL	H	2	4	• “And actually was a little disappointed when the Patriot Act was ah, I think if I'm not mistaken, I know it's being re-looked, I think it may have been approved, but I'm not sure we've made any adjustments on that. For our, our, our new um for this period, any updates, if you will, excuse me." (11224014306, REGL05, DTVP) • “Um um but but looking at the some of the previous models, um especially with uh Chelsea Manning, and and uh and others. Um it it certainly did harmful and uh severe damage to the US government writ large." (11251351842, REGL01, SIPC)
H1/SPCN	H	3	8	• “I become quite concerned, also concerned with little funny things that happen when ah I'm standing around talking about a subject and it shows up on my ah Amazon feed or something of that nature." (11224014306, SPCN08, DTVP) • “Okay, yeah, that was a surprise to me. Um, I, at first I was I was uh, I was quite unhappy about that. But on the other end, I went back to my original philosophy. Well, I put the stuff out there." (11205114603, SPCN04, SIPC)

(continued)

Hypo/ Code	OG	Participants	Snippets	Representative Snippets
H1/USGE	H	3	7	• "So ah somebody's grabbing my information, ah somebody's using it for whether it's sales, or whether to rob me or use my uh uh social security number." (11224014306, USGE12, DTVP) • "Uh, for whatever purposes um, you know, could be nefarious, it could simply be trying to find the right people for the right position across the IC uh or other other agencies, private and public." (11205114603, USGE10, SIPC)
H2/CNTL	A	1	7	• "Okay. So once again, I mean it's, it's up to me to be careful of what I put out there in terms of uh you know what content I make available." (11269613365, CNTL12, SIPC) • "If I'm worried about it, it's gonna be a situation where I'll push it to the guy. And it won't be through the site, it'll be through an email or something a little bit more secure." (11269613365, CNTL11, BITN)
H2/PRBF	A	2	6	• "So, you know, again uh, you know, I made the conscious effort, uh the conscious decision that that what they were going to be able to ascertain from me was uh not going to directly uh um affect me and uh in a negative way and and not to negatively uh affect me in an indirect ways either. Um I don't think that a uh bad actor could um necessarily get enough information to do do me or my um family harm." (11188138618, PRBF14, SIPC) • "I also realize that people that know know people that I know can see my some of my stuff because they, they share it. So, once again, I uh it's my assumption that anything that's on those sites is going to be open source to anybody." (11269613365, PRBF11, BITN)
H2/USGE	A	2	3	• "Uh I believe that IC I don't know where ICWATCH is located or the people that are involved in it, but they potentially make it easy for enemies of the United States to assemble information." (11223476508, USGE09, SIPC) • "And I believe that uh people generally generally are doing the right thing and abiding by the terms of service and uh and why they're using the system. But I know that that is not always the case." (11223476508, USGE06, BITN)
H2/BEHV	H	3	6	• "And I think I went back there and uh did a general scrub and use more general terminology, because I'm not I'm no longer in that in that profession." (11205114603, personal communication, BEHV02, SIPC) • "So I I toned that thing down. An I uh think I uh I uh may be doing the same with uh LinkedIn." (11224014306, BEHV03, BITN)

(continued)

Hypo/ Code	OG	Participants	Snippets	Representative Snippets
H2/COLL	H	1	3	• “So uh I think I need some questions answered, um before I can move forward in having worked in the IC community for a short period of time, just a couple years, I know the capabilities of what they can do and and uh things they can look at." (11224014306, COLL05, SIPC) • “Um again, I don't know, they're we're looking at if they've taken everything, um IP addresses, any phone numbers that may or may not be in there. Anything, anything I may have said." (11224014306, COLL08, BITN)
H2/ERRS	H	1	2	• “But uh, but for me, I have no need to be in that um in that world anymore. Uh, so as time goes on I, I remove a lot of those specific key terminologies simply because um that's in the past and it's no longer relevant." (11205114603, ERRS03, SIPC) • “Um, as I mentioned before, I'm definitely uh steering away from uh the IC community because uh I haven't been involved in in quite a while there's really no point it's actually misleading. For those who see that language. Um, I don't want to waste anybody's time. And uh really, um but it's it's a constant care and feeding of my public profile to present the most accurate up to date and uh harmless um public presentation that I can um you uh to uh you know benefit those in my network and uh and myself to be honest." (11205114603, ERRS02, BITN)

Note. Codes for behavior and SPCN, which directly reflect the underlying constructs and topics, support/refute the associated hypotheses. Only one participant provided a single snippet for COLL or ERRS in SIPC, accounting for the duplication. Snippet details provided after each in the following format: Participant ID, Code ID, Category. Code ERRS03 intentionally used twice.

There were no codes shared between the two groups; six codes were overlapped within the groups (collection control, errors, PRBF, regulations, and usage) and across the categories, with 66.67% participant representation in four (control, PRBF, regulations, and usage). Both groups also overlapped on the code SPCN, which reflects statements directly related to one of the hypothesis constructs and discussion topics, with a 66.67% representation. There was overlap on two codes for group A, indicating that decisions on what/when to share (control) and expectations of privacy on sites (PRBF) may antecede or moderate this hypothesis for the lesser degree representation group, with

100% of participants for control and 66.67% for PRBF. There was overlap on five codes for group H (collection, errors, regulation, SPCN, and usage) for the higher degree representation group, with 100% of participants for both SPCN and usage, each having the second-largest number of snippets, eight and seven, respectively. Support for regulation was at the 66.67% participation level.

Group H indicated both knowledge of internet collection and analysis activities (collection) and notions about inaccuracies (errors), but a single participant only presented each with a single snippet. This would indicate that these were not relevant factors in the higher degree representations of the variables.

Hypothesis Two (H2). The quantitative analysis found significant support for H2, showing that SIPC has a negative effect on the intention (BITN) to continue sharing information publicly on LinkedIn. Table 14 details the findings for the integration of results associated with H2. Overlap analysis of categories SIPC and BITN resulted in six codes supported by 27 snippets presented from all six participants.

Again, there were no codes shared between the two groups; five codes were overlapped within the groups (collection, control, errors, PRBF, and usage) and across categories, with 66.67% representation in two code, PRBF and usage. Both groups also overlapped on the code behavior, reflecting statements directly related to one of the hypothesis constructs and discussion topics, with an 83.34% representation. There was a 50/50 split of the six associated codes between the two groups. There was overlap on three codes for group A (control, PRBF, and usage), which may antecede or moderate this hypothesis for the lower degree representation group, with 66.67% of participants for both PRBF and usage. There was also overlap on three codes for group H (behavior, collection, and errors) for the higher degree representation group, with 100% of participants for behavior.

There was overlap on one code for group A, indicating that decisions on what/when to share (control), but a single participant only presented each with a single snippet. This would indicate that these were not substantial factors in the higher degree representations of the variables. The same outliers for group H associated with Hypothesis One (H1) also apply here, single contributions for both collection and errors.

Summary of Results

The mixed methodology approach produced two datasets, quantitative and qualitative, which were then integrated. The following summarizes whether the hypotheses were supported and significant, which other factors potentially underlie the study's unidimensional constructs, and which other factors potentially influenced the hypotheses.

Constructs

Breach of privacy. 66.68% of the participants did not indicate they believed this to be a breach of privacy. When discussed, both groups indicated that this might be more relevant to privacy risk beliefs (66.67%) and general privacy concerns (33.33%). However, the groups diverged on other influencing factors. Two-thirds of group A implied that control might influence this. Two-thirds of group H implied that several other factors might influence this, including benefit, collection, invasion, situational privacy concern, and usage.

DTVP. When discussed, only 66.67% of the participants affirmed privacy concerns (GPCN); however, both groups indicated the influence of benefit (33.33%), control

(66.667%), and PRBF (50.00%). However, group H at 66.67% representation indicated that specific (SPCN) versus general privacy concerns may be meaningful in the lower degree of the variables.

SIPC. When discussed, both groups indicated that this might be influenced by collection (50.00%) and usage (66.667%). However, the groups diverged on other influencing factors. Additionally, group A at 66.67% representation indicated that usage may be important in the lower degree of the variables. All members of Group H made reflective statements regarding SPCN bolstering support in the higher degree of the variables.

BITN. When discussed, both groups at 100% of all participants indicated that the advantages of having a profile (benefit) might be influential. However, only 83.33% of all participants discussed their intentions to modify their profile (behavior, with only group H affirming this intent). Additionally, group A at 66.67% representation indicated that usage may be meaningful in the lower degree representations of the variables.

Supplementary. When allowed to provide additional reflections not explicitly related to any topic, the groups diverged on other influencing factors. Group A indicated, with 66.67% representation, that control and PRBF may be meaningful in the lower degree representations of the variables. However, group H indicated, with 66.67% representation, that regulations may be meaningful in the higher degree representations of the variables.

Hypotheses

Hypothesis One (H1). H1 had significant support and showed that DTVP influenced SIPC as expected. However, the groups diverged on potential influencing factors. Group

A had two shared codes bridging the hypothesis constructs, control (100%) and PRBF (66.667%). Group H also had three shared codes, regulation (66.67%) and usage (100%), as well as SPCN (100%), which was reflective of both a construct and topic.

Hypothesis Two (H2). H2 had significant support and showed that SIPC did influence BITN as expected. Again, the groups diverged on potential influencing factors. Group A had two shared codes bridging the hypothesis constructs, PRBF (66.67%) and usage (66.67%). Group H only had one code behavior (100%), indicating their unanimity towards modifying their profile.

Control variables. Neither of the control variables, age or sex, influenced BITN. However, not all categories could be analyzed due to sampling limitations.

Chapter 5

Conclusions, Implications, Recommendations, Summary

The chapter presents the conclusions drawn from the mixed methods design and subsequent findings, providing a discussion on accomplishing the objectives, alternative explanations, strengths, weaknesses, and limitations. From there, an elaboration of the findings' implications regarding their contributions and impacts on the field of study. Then, it furnishes recommendations for future research and the application to professional practice. Finally, the chapter culminates in a full summary of the research study.

Conclusions

The mixed method approach was completed in two phases. The quantitative portion utilized a survey instrument and PLS model analysis, while the qualitative portion used interviews followed by sequential integration. Overall, the analysis showed clear support for the underlying research questions, all of which were grounded in the context of providing empirical justification for a relationship between privacy concern and behavior intention in an actual privacy-centric situation. The second phase of the mixed method approach provided context to the research questions, resulting in strong representation for several antecedents or moderating factors, often spread unequally across the two groups characterizing the low and high degree of variable representations. Across the entire situation, participants in group A (lower degree of variables) presented the only factor (privacy risk belief) that bridged across both hypotheses. It was evident that more factors influenced group H participants (higher degree of variables), presenting all 12 codes, five more than group A. Group H appeared to be additionally influenced by factors such as the inaccuracy of their information (errors), negative experiences on the Internet (invasion), their personality quirks (personality traits), existing laws (regulations), and concerns about ICWATCH or the situation (specific privacy concerns).

When allowed to provide additional reflections not explicitly related to any topic, both groups were again divided on the underlying factors influencing the situation. Group A again commented on the influence of choosing what to share (control, 66.67%) and the expectation of privacy on LinkedIn (privacy risk belief, 66.67%). Group H also reiterated that influences regarding applicable laws (regulation, 66.67%) were still present. Lastly, for each of the hypotheses, the groups continued to diverge on the underlying factors.

The two groups personified the opposite degrees of the relationships between the hypothesis variables. The only exact point of agreement between the two groups was the advantages of having a LinkedIn profile. Group A members had the least concern for privacy in general and none with the situation and had no plans nor intention to change their profile. Their ability to select what, when, and where to share was the most expressed, at 10 times the amount of comments of their counterparts. While they knew their information was being collected on the internet, they did not expect privacy.

On the other hand, group H members valued the right to be left alone. They were concerned when they saw this situation and expressed an intent to "tone it down" (profile) or "take another look." They also revealed more latent factors influencing both their privacy concerns and subsequent profile changes. These factors included that their profile may not reflect their current resume accurately. They had previously had an account hacked, or money was stolen. They were introverted or uninteresting, or they were not sure that protections provided by laws and regulations (e.g., Patriot and Privacy Acts) were enough. They acknowledged that there was no expectation of privacy on the internet, but at four times as much as their counterparts. While they also knew their data was being collected and had no expectation of privacy, they expressed these sentiments at twice their counterparts' rate.

Hypothesis One (H1)

The quantitative analysis showed strong support for the first hypothesis, that general privacy concerns influence situation-specific privacy concerns in actual privacy-centric situations. Again, different factors were exposed to be either antecedent or moderating between the different degrees of each associated variable. Group A expressed support for the influence of both control and privacy risk belief (66.67%). Participants in this group expressed a conscious choice to both participate and what information to share on LinkedIn (control), as expressed by Participant 11188138618, "…if I want to be private, that I don't engage … that's the only way to be completely private." They also expressed sentiments regarding the conscious decisions made when posting information to LinkedIn and that the data was either already sanitized appropriately or not sensitive (privacy risk belief); as voiced by Participant 11188138618, "…I made the conscious effort, uh the conscious decision … I don't think that a uh bad actor could um necessarily get enough information to … do me or my um family harm."

Group H conveyed support for the influence of regulation (66.67%), specific privacy concerns (100%), and usage (100%). Participants in this group indicated the apparent lack of application of existing regulations (Constitutional amendments, Patriot Act, and Privacy Act), as well as a lack of government action (regulation), as disclosed by Participant 11251351842, "… the fact that ICWATCH has violated personal privacy in the past … the US Government's [lack of] resolve to do anything about it." They also expressed concern when they became aware of the situation (specific privacy concerns), as revealed by Participant 11251351842, "… their [ICWATCH] behavior certainly raises red flags." Finally, they indicated a lack of understanding as to what ICWATCH was doing with their data, expressing that it may be inappropriate (usage), as expressed by Participant 11224014306, "… if I'd summed up in one statement, what are you [ICWATCH] doing with it?"

Hypothesis Two (H2)

The quantitative analysis also showed strong support for the second hypothesis, that situation-specific privacy concerns influence behavior intention in actual privacy-centric situations, again with diverging underlying factors. Group A indicated support for the influence of both privacy risk belief (66.67%) and usage (66.67%). Participants in this group indicated that a conscious choice was made to post information they knew could be shared and seen by others, and the risk had been evaluated (privacy risk belief), as disclosed by Participant 11269613365, "… it's my assumption that anything that's on those sites is going to be open source to anybody." They also expressed notions indicating they recognized their data was probably being used in ways they did not fully understand (usage), as voiced by Participant 11223476508, "And I believe that uh people … are doing the right thing and abiding by the terms of service …. but I know that that is not always the case." All Group H members were like-minded in that they already had or planned to revisit their profile on LinkedIn, as expressed by Participant 11205114603, ″…. I plan on I don't do it as frequently as I should. …. But yeah, before the weekend. I'll probably go back in there [LinkedIn]."

Breach of Privacy

It was clear that while this was a privacy-centric situation that was of privacy concern, it was not a breach of privacy. When discussed, both groups indicated an influence by privacy risk beliefs (66.67%). Participants in both groups indicated that there was no expectation of privacy, as people are essentially putting their information in the public domain (privacy risk belief), as disclosed by Participant 11269613365, "But I think if you go out to social media sites … you don't have any uh, any expectation of privacy at that point." (11269613365, personal communication, March 28, 2020). However, the groups differed on other elements. Group A conveyed support for the influence of control (66.67%) in that participants could choose what to share, as voiced by Participant 11223476508, "… my resume is an assemblage of my life experience and I have not divulged any classified information. In fact, that resume was scrubbed and approved for release prior to it being posted anywhere or used for my job search."

However, Group H indicated support for the influence of collection (66.67%) and usage (66.67%). Participants noted the potential naïveté of Internet users (collection) and the sophistication of Internet aggregation, as indicated by Participant 11205114603, "...I'm not sure many people realize that whatever they put out there is being scooped up ... to assist whatever agency creates those aggregators." They also conveyed that providers and others are using data without permission and for undesirable and/or unknown purposes, as revealed by Participant 11251351842, "… takes that information and uh puts it in, in the public under a false light … for some sort of uh, uh commercial advantage."

Constructs

The qualitative findings also provided insight into each of the antecedents or moderators of the individual constructs. For DTVP, both groups indicated the underlying influence of both the decision of when/what to share (control, 66.67%) and the expectation of losing privacy on LinkedIn (PRBF, 50.0%), with 66.67% making statements reflective of their inclination to worry about privacy (GPCN). However, group H indicated that associated laws (regulations, 66.67%) and concerns regarding the ICWATCH situation (SPCN, 66.67%) also exert influence. For SIPC, both groups indicated that this was influenced by their information being collected and analyzed (collection, 50.0%) and what purposes their data was being used for (usage, 66.667%). Consistent with the trend, the groups diverged on other influencing factors. Group A described the influence of PRBF (66.67%), while 100% of group H made comments directly reflective of situational privacy concerns (SPCN). For BITN, both groups indicated the influence regarding the advantages of the data available in the profile (benefit, 100%), with 83.33% discussing their choice to modify their profile (behavior). However, group A also implied that ambiguity regarding how the data was employed (usage, 66.67%) influenced their perspective.

Objectives

The results of the study met the three goals associated with the research. The first goal was that the research would contribute to the literature by providing empirical justification for a relationship between privacy concerns and behavior intention in an actual privacy-centric situation. As in the literature, the results demonstrated that the resulting significance was similar, whether applied to an actual situation or contrived scenarios. For Hypothesis One (H1) DTVP→SIPC, this study found a $p<.001$ significance. Kayhan & Davis (2016) and Li (2014) found similar levels of significance for similar constructs, $p<.01$ and $p<.05$ levels, respectively. For Hypothesis Two (H2), SIPC→BITN, this study found a $p<.001$, which was similar to that found by Li (2014) at $p<.01$. The second and third goals were that the research would justify the appropriateness of the constructs and scales regarding usage in actual situations. With valid findings for the research model analysis and tests of measurement items, the constructs and scales remain valid and applicable in an actual context. The qualitative results provided further justification as each construct was equated with a category and discussed with participants, with no noted issues. The author informed interview participants at the outset that they could ask for clarification at any time and was provided the opportunity to add additional reflections at the end, yet did not.

Alternative Explanations

Other factors may have contributed to findings of which privacy concerns were only antecedent or moderating. The sentiments expressed regarding the advantages of sharing information on LinkedIn (benefit) had 100% representation by all the interview participants. The population for the study consisted of 1st- and 2nd-degree LinkedIn connections to the author. A potential population skew existed as there was no way to determine which profiles resulted from LinkedIn searches, considering both the multitude of factors associated with any individual's profile (e.g., sex, age, education, industry, number of connections, etc.) and no insight into the search algorithm itself.

Limited participation may have also skewed the results in real privacy-centric situations. The participation of only 65 out of 1,310 (4.96%) possible responders to complete the survey and 44 volunteering for follow-up interviews (3.35%) may not be surprising. Only the most concerned individuals may have volunteered (i.e., the most robust representation of the variable), accounting for the lack of representation in other outcome groups. Males overrepresented females by 612.50%, and the age category of older than 50 years overrepresented all other age categories combined by 50%. Chakraborty et al.'s (2013) work was indicative of this response. His work on Facebook found partial support for older males and females, making different sharing decisions. Similarly, Zhang et al. (2013) discovered a positive correlation between age and privacy concerns (multidimensional; in an m-commerce context), as well as support for age influencing behavior (specifically younger users' willingness to conduct mobile commerce [m-commerce] activities). Either or both of these could account for the significance of the findings.

Strengths, Weaknesses, Limitations

Strengths. While not a breach of privacy, both groups' revelations of their expectation of losing privacy on LinkedIn (privacy risk belief) supports labeling this situation as privacy-centric. The qualitative codes were operationalized using items adapted from validated constructs in the existing literature. This alignment was appropriate as this study sought to validate the unidimensional privacy concerns, which resulted in evidence of the multidimensional aspects during descriptive analysis. Moreover, the increase of significance from contrived scenarios (*p*<.05 and *p*<.01) to actual (*p*<.001) bolstered the validity of the findings.

Weaknesses. The study utilized a convenience population, limiting the generalizability of results, which was exacerbated by a sample size of only 65 (a 4.96% participation rate) and skewed heavily towards men over 50 years of age. The interview methodology front-loaded the breach of privacy topic at the onset of the interview. While necessary to validate the research's underlying assumption, it may have framed the discussion, thereby skewing the presented factors and the final qualitative results. While only two outcome groups reached the 5% level, other non-represented outcome groups may have presented different unique factors during the interviews, changing the factors underlying each hypothesis. Four codes were represented weakly across all six interview participants, errors (16.67%), invasion (33.34%), PNTR (16.67%), and regulations (33.34%), which may have been more weighty with more participants. Lastly, while group H presented homogenously for both SPCN (100%) and usage (100%), several snippets had qualifiers indicating that it was not surprising upon reflection, as revealed by Participant 11205114603, "… the more I thought about it, the more I realized, well, that's to be expected."

Limitations. Access to demographic diversity may continue to be problematic in real situations. For this study, the Intelligence Community was the target of the privacy-centric situation; however, of the 16 agencies comprising the Intelligence Community, more than half (9) fell under the Department of Defense (DoD) (Office of the Director of National Intelligence [ODNI], n.d.). Considering this, approximately 16% of the active-duty force (Air Force, Army, Marines, Navy) are female (Defense.gov, n.d.). Next, assessing actual behavior, not merely intention, may be problematic. Initially, the deployed methodology only assessed if participants modified their profiles; actual behavior regarding privacy concerns had little representation in the literature. However, once LinkedIn changed its security settings, the author lacked a viable way to validate that while the hypothesis was supported, people subsequently modified their profile. Also, locating actual privacy-centric situations and their identifiable populations is problematic as well. The study focused on a specific situation, which could infer the findings were only relevant in this particular instance. Finally, no specific methodology approximated the population demographics at the onset. Informally, the author assumed that the age and sex of the population would be equally distributed. Such was not supported in this study.

Implications

This research provides valuable contributions to the existing literature gaps regarding general and specific privacy concerns and their influence on behavior intention in a real situation. In contrast, the literature is primarily based on studies using contrived approaches. This study used individuals in actual situations and evaluated their behavioral intention on a specific action available to them.

The results provide empirical support for the influence of other factors in actual privacy-centric situations. As there may be limited opportunities to investigate actual privacy-centric situations, underlying factors expressed here lend support to prioritizing them over others. For instance, benefit was the only factor presented by all six participants.

An assumption that researchers need to find a breach of privacy to best model a privacy-centric situation may not be necessary. Qualitative findings indicated a breach was not required. Support for the hypotheses and associated qualitative factors only indicate that situations be privacy-centric. The findings also support utilizing multidimensional constructs for privacy concerns in actual situations versus unidimensional. This study modeled the literature trend of broad to specific and found good support for a unidimensional application. However, the qualitative portion revealed factors such as collection, invasion, errors, and usage, which typically align with multidimensional privacy concerns, such as CFIP. There was a lack of overlap in the shared codes across the two hypotheses and only full participant support for one code, implying that various factors may influence the entire situation. Compounding this possible scenario is that each group, representing different degrees of the variables, presented different codes for each hypothesis, with only a single code (PRBF) bridging for the low representation of the variables.

The results also have implications for the populations associated with research on actual privacy situations regarding demographics and participation. The general assumption that a relatively equal distribution of sex and age will be available is likely not realistic in real situations. As these situations are unpredictable, researchers may need to aggregate individual cases to accommodate diverse demographics fully. The necessary rate of participation may also pose challenges. Although 78 individuals were willing to engage at some level, which implies that these situations can yield viable populations, it may be unpredictable. As Participant 11269613365 stated, "I don't friend everybody asked to be friended …. I don't if I don't know the person."

Research into actual privacy situations may need to modify participation assumptions to accommodate lower participation rates. This study expected a participation rate of 19% using LinkedIn, based on results from Claybaugh and Haseman (2015), yet only achieved a 4.96% rate.

Recommendations

Based on this study's population demographics, future researchers may want to over-sample a specific demographic intentionally to compensate for a lower participation rate, as was the case in this study, with women participation at just 6.04%. While not an entirely reliable method, something akin to the post-population analysis using popular baby names, could help ensure a more equitable participation distribution. Xu, Dinev et al. (2011) noted that using a more diverse sample increased generalizability to the general population.

Actual privacy situations require further research. While the findings support the hypotheses in this real privacy-centric situation, additional studies should address if the results are unique to this particular situation. Applying a mixed method approach would also address whether the same qualitative factors are present or changed in different situations. Future studies using a mixed method approach should also consider using a more open interview process. While a semi-structured approach was a reasonable trade-off between structured and open for this initial study into an actual situation, an open interview process may have revealed other latent factors.

While all group H members presented supportive codes for both behavior and SPCN as expected, research into actual situations should consider prioritizing the latent factors of benefit and usage, which also had 100% representation. While the groups representing different degrees of the variables diverged on provided codes, prioritizing the higher degree group's factors should be considered. From a full model perspective, the advantages (benefit) in having a LinkedIn profile may indicate a privacy paradox for participants (Wakefield, 2013; Xu, Luo et al., 2011). While it did not factor directly into the hypothesis support, this high degree of representation suggests its influence, as expressed by Participant 11269613365, "So that to me is a social media site's all about us out there trying to basically generate a network."

For OSN providers, the results indicate that while the participants did not express an intention to discontinue using the platform, it was evident that external actors may influence what information they choose to share/continue sharing based on external visibility. As noted by Kayhan & Davis (2016), "Increased awareness of the factors that contribute to situational privacy concerns will enable online service providers to be more proactive in mitigating concerns" (p. 233).

Summary of Results

Both the government and large public organizations (i.e., Google, Facebook, and Amazon) have recently encountered news-worthy privacy issues regarding the massive amounts of data each collects, transmits, and stores. However, private entities, such as ICWATCH, also use available information for profiling purposes. Multiple studies have explored both the contextual and situational aspects of privacy, as well as its paradoxical nature. However, there remains a gap in understanding if the influence of privacy concerns on behavior intention can be extended to actual situations, especially since an individual's behavior related to privacy concerns can be unpredictable.

This study had three goals focused on extending the existing literature onto an actual privacy-centric situation. Specifically, providing empirical justification for the established relationship between privacy concern and behavior intention, appropriateness of existing constructs, and suitability of existing scales. The study also sought to answer three research questions grounded in an actual situation. First, what is the user's disposition towards privacy? Second, to what extent does this influence users' privacy concerns regarding the inclusion of their LinkedIn profile information within ICWATCH? Third, to what extent do these concerns influence their stated intention to modify their LinkedIn profile/settings to minimize/eliminate this inclusion?

The study was relevant as it progressed the field into an actual situation and modeled the broad to specific approach in the existing literature. Researchers poorly understood these underlying problems in the context of an actual situation. It was not clear what other factors might influence findings from previous research. This study was unique. It evaluated what participants declared they would do (well covered in the literature) but what individuals might do in the context of an actual privacy-centric situation (little coverage in literature). Opportunities to study real privacy-centric situations are problematic as such situations are ad-hoc in nature, and affected populations may not be identified easily.

A few issues were evident from the privacy literature. A variety of factors influence privacy concerns and apprehension regarding the use of convenience populations. The author assumed that users were unaware of this situation. As such, it was appropriate to evaluate privacy concerns as a unidimensional construct and that the actual situation qualified as privacy-centric. The researcher identified two limitations associated with the research. The reliance on external services (i.e., LinkedIn and ICWATCH) and new/ongoing Internet security events might influence the study. This cautious approach constrained the research scope by limiting it to a single behavior, two control variables (age and sex), two degrees of connections via LinkedIn, and a 30-day window disqualifier question.

The research included three constructs well represented in the literature, disposition to value privacy, situation-specific Internet privacy concerns, and behavior intention. The study included both privacy concern constructs as unidimensional in order to model the broad-to-specific approach, even though multidimensional privacy concern constructs were available (i.e., CIFP and IUIPC). The construct for behavior was specifically narrowed to intention (i.e., future action), ignoring both current and past variations. This study's strength rested with its underlying foundation of consistent results from the utilized scales, constructs, and methodologies in the literature. The relevant gap was the minimal investigation grounded in actual situational influences associated with privacy concerns and behavior.

The research design employed an explanatory sequential mixed methods design with interview follow-up, which involved collecting quantitative data first and then contextualized the quantitative results with qualitative data. The first quantitative phase of the study used survey methodology. The instrument variables were operationalized using items adapted from validated scales, with items re-worded to fit the research context. The researcher measured each of the three constructs with a seven-point scale, the control variables by a single item each, with an additional binary scale question as a participant disqualifier. Initial discovery methodology validated a viable population on

LinkedIn before administering the survey to 1,310 individuals thru LinkedIn directly. There were 65 valid responses, resulting in a 4.96% participation rate, heavily skewed towards males (87.69%) over 50 years of age (60.00%).

The second qualitative phase of the study utilized follow-up semi-structured interviews. The interview, structured around four topics aligned to assumptions or constructs in the research, was supplemented with a fifth category to capture participants' reflections. The valid survey respondents from the previous phase, who indicated a willingness to participate, comprised the interview population. Survey participants were assigned to one of eight possible outcome groups, characterizing each variable's least ambiguous representation derived from a simple scoring model. The researcher invited the most representative scoring participants for follow-up interviews from the only two groups meeting the established 5% sample threshold per group. Six participants, all-male and over 50, were interviewed from two groups representing different degrees of variables (i.e., less/more concerned and not likely/likely to modify profile). The resulting snippets were analyzed and aligned with 12 codes, operationalized with existing constructs in the literature. After a code-snippet validation, the resulting data set was 139 code-snippet pairs.

The quantitative phase utilized SmartPLS to perform the partial least squares analysis and derive both the measurement and structural model findings. A second software solution called G*Power indicated that 65 samples were enough for PLS analysis, calculating that 62 was the minimum threshold. The measurement model analysis assessed both the convergent and discriminant validity and reliability, with all results exceeding the required thresholds. The structural model analysis revealed that Hypothesis

One (H1) had significant support that DTVP did influence SIPC as expected. Hypothesis Two (H2) also had significant support showing that SIPC did influence BITN as expected. However, there was no significance for any influence of either age or sex on behavior intention, although neither could be modeled fully.

The qualitative phase utilized sequential integration to contextualize the findings from the previous phase. First, the author mapped each of the code-snippet pairs to the topics and constructs and noted observations and outliers. The majority of participants did not indicate a breach of privacy with shared expressions on the influence of privacy risk belief and general privacy concerns, and diverging opinions across seven other factors. Both groups also indicated that DTVP might be influenced by benefit, control, and privacy risk beliefs and diverged on the influence of specific privacy concerns. Both groups indicated that SIPC might be influenced by collection and usage and diverged on two other factors. Lastly, both groups indicated that BITN might be influenced by benefit but diverged on the influence of usage.

Next, shared code-snippet pairs between each hypothesis were mapped, and observations and outliers were noted; however, there were no shared codes between the two groups on either hypothesis. For Hypothesis One (H1), the lesser degree group expressed the influence of control and privacy risk beliefs, while the higher group indicted regulation and usage. For Hypothesis Two (H2), the lesser degree group indicated that privacy risk belief and usage might have influence. Only one shared code (privacy risk beliefs) was shared across the lesser degree group's hypotheses.

Ultimately, the results of the study showed both support for the hypotheses and the existing literature. Those participants who were neither inclined to privacy nor concerned with the situation did not intend to modify their LinkedIn profile; however, they indicated that control and privacy risk belief might exert influence. Those participants who were more inclined and more concerned about the situation did express an intent to modify their profile and revealed influencing factors such as regulations and usage. The results provided empirical justification for the established relationship between privacy concern and behavior intention, appropriateness of existing constructs, and suitability of existing scales in an actual situation. The methodology and results also revealed challenges with achieving population demographic equitability when investigating actual privacy-centric situations. Finally, the qualitative findings established a foundation for using multidimensional scales and prioritizing other constructs, such as benefit, when investigating actual privacy situations.

Appendix A

Supporting Tables

Table A1

Research Contributions Based on Variable Outcomes

Outcome-Group	**BITN(-)**	**DTVP(+)**	**SIPC(+)**	**Contribution**
OG-A	H	L	L	*Full hypothesis support.* The participant indicated they were more likely to continue sharing their profile, as they were both less disposed to value privacy and less concerned about the situation. Interviews may expose influencing factors, underrepresented in current research, which are only apparent in an actual privacy-centric situation.
OG-B	L	L	L	*Partial hypothesis support.* The participant indicated they were more likely to stop sharing their profile even though they were both less disposed to value privacy and less concerned about the situation. Interviews may help explain the contradictory findings for the established relationship between SPC > BITN.
OG-C	H	L	H	*No hypothesis support.* The participant indicated they were more likely to continue sharing their profile as they were less disposed to value privacy and yet, more concerned about the situation. Interviews may help explain the contradictory findings between the established relationships for both DTVP > SPC, as well as SPC > BITN.
OG-D	L	L	H	*Partial hypothesis support.* The participant indicated they were more likely to stop sharing their profile, even though they were less disposed to value privacy and yet more concerned about the situation. Interviews may help explain the contradictory findings between DTVP > SPC.

(continued)

Outcome-Group	**BITN(-)**	**DTVP(+)**	**SIPC(+)**	**Contribution**
OG-E	H	H	L	*Partial hypothesis support.* The participant indicated they were more likely to continue sharing their profile, even though they were more disposed to value privacy and yet less concerned about the situation. Interviews may help explain the contradictory findings between DTVP > SPC.
OG-F	L	H	L	*No hypothesis support.* The participant indicated they were more likely to stop sharing their profile as they were more disposed to value privacy and yet less concerned about the situation. Interviews may help explain the contradictory findings between the established relationships for both DTVP > SPC, as well as SPC > BITN.
OG-G	H	H	H	*Partial hypothesis support.* The participant indicated they were more likely to continue sharing their profile even though they were both more disposed to value privacy and more concerned about the situation. Interviews may help explain the contradictory findings between SPC > BITN.
OG-H	L	H	H	*Full hypothesis support.* The participant indicated they were more likely to stop sharing their profile as they were both more disposed to value privacy and more concerned about the situation. Interviews may expose influencing factors, underrepresented in current research, which are only apparent in an actual privacy-centric situation.

Note. H = high score, L = low score

Table A2

Theories in Privacy Research

Theory	Synopsis	Relation to Privacy Concern Category	Reference Studies
Agency Theory	The relationship between the principal whom delegates actions to an agent; specifically, conflict in desires and goals, and/or validation of the agent's actions	Origin of privacy concerns Text	Xu, 2010
Social Contract Theory	The social norms shared between two parties and their associated rights and responsibilities		Li et al., 2010
Theory of Reasoned Action (TRA) and Theory of Planned Behavior (TBP)	Beliefs and attitudes determine behavior; TBP adds behavioral control as a factor	Behavioral consequences	Bansal et al., 2016; Dinev & Hart, 2006
Privacy Calculus (including Utility maximization, expectancy theory of motivation, Expectancy-value theory)	Behavior is based on a performed calculus based on weighed factors	Trade-offs	Bansal et al., 2010; Bansal et al., 2016; Cichy et al., 2014; Dinev et al., 2008; Li et al., 2011; Li, 2014; Miltgen & Peyrat-Guilard, 2014; Min & Kim, 2015
Procedural Fairness Theory	Fairness (aka justice) intermediates in the trust between principals and agents, in that the actions taken on behalf of the principal should be transparent	Institutional influential factors	Xu, Dinev et al., 2011

(continued)

Theory	**Synopsis**	**Relation to Privacy Concern Category**	**Reference Studies**
Protection Motivation Theory	Fear appeals on attitudes and behaviors from specific threats and coping evaluations	Individual influential factors	Zhang et al., 2018
Information Boundary Theory	A calculus generating rules for disclosing information from a cost-benefit perspective across individual privacy boundaries		Choi & Land, 2016; Xu, Dinev et al., 2011
personality theories	Personality traits influence privacy behaviors		Li, 2014; Osatuyi, 2015

Note. Adapted from Li, Y. (2012) Theories in online information research: A critical review and an integrated framework, *Decision Support Systems, 54*(1), p. 474

Table A3

DTVP Measurement Items

Reference	Question 1	Question 2	Question 3
Kayhan & Davis, 2016 (p. 236)	“Compared to others, I am more sensitive about the way my personal information is handled.”	“Compared to others, it is more important for me to keep my information private.”	“Compared to others, I tend to be more concerned about threats to my information privacy.”
Li, 2104 (p. 353)	“Compared to others, I am more sensitive about the way other people or organizations handle my personal information.”	“Compared to others, I see more importance in keeping personal information private.”	“Compared to others, I am less concerned about potential threats to my personal privacy. (reverse-worded)”
Li et al., 2011 (p. 443)	“Compared to others, I am more sensitive about the way online companies handle my personal information.”	“To me, it is most important to keep my privacy intact from online companies.”	“I am concerned about threats to my personal privacy today.”
Li et al., 2017 (p. 1021)	“Compared to others, I am more sensitive about the way online companies handle my personal information.”	“To me, it is most important to keep my privacy intact from online companies.”	“I am concerned about threats to my personal privacy today.”
Malhotra et al., 2004 (p. 352)	“Compared to others, I am more sensitive about the way online companies handle my personal information.”	“To me, it is the most important thing to keep my privacy intact from online companies.”	“I am concerned about threats to my personal privacy today.”
Xu, Dinev et al., 2011 (p. 823)	“Compared to others, I am more sensitive about the way companies handle my personal information.”	“To me, it is the most important thing to keep my information privacy.”	“Compared to others, I tend to be more concerned about threats to my information privacy.”

Note. Seven-point scales anchored with “strongly disagree” and “strongly agree.”

Table A4

Situation-Specific Internet Privacy Concern Measurement Items

Reference	Question 1	Question 2	Question 3	Question 4
Dinev & Hart, 2006 (p. 77)	"In general, I am concerned that the information I submit on the Internet could be misused."	"In general, I am concerned that a person can find private information about me on the Internet."	"I am concerned about submitting information on the Internet, because of what others might do with it."	"In general, I am concerned about submitting information on the Internet, because it could be used in a way I did not foresee."
Min & Kim, 2015 (p. 857)	"I am concerned that the information I submit on Facebook could be misused."	"I am concerned that a person can find private information about me on Facebook."	"I am concerned about submitting information on Facebook, because of what others might do with it."	"I am concerned about submitting information on Facebook, because it could be used in a way I did not foresee."
Ozdemir et al., 2017 (p. 658)	"I am concerned that the information I share through the Internet with people I know could be misused by them."		"I am concerned about sharing information through the Internet with people I know, because of what they might do with it."	"I am concerned about sharing information through the Internet with people I know, because they could use it in a way I did not foresee."
Son & Kim, 2008 (p. 526)	"I am concerned that the information I submit to online companies could be misused."	"In general, I am concerned that a person can find private information about me on the Internet."	"I am concerned about providing personal information to online companies, because of what others might do with it."	"I am concerned about providing personal information to online companies, because it could be used in a way I did not foresee."

(continued)

Reference	Question 1	Question 2	Question 3	Question 4
Xu et al., 2011 (p. 823)	"I am concerned that the information I submit to this website could be misused."	"I am concerned that others can find private information about me from this website."	"I am concerned about providing personal information to this website, because of what others might do with it."	"I am concerned about providing personal information to this website, because it could be used in a way I did not foresee."

Note. A mixture of five-point (Dinev & Hart, 2006; Ozdemir et al., 2017) and seven-point (Min & Kim; Son & Kim; Xu, Dinev et al., 2011) scales anchored with "strongly disagree" and "strongly agree."

Table A5

Behavioral Intention Measurement Items

Reference	Question 1	Question 2	Question 3
"The extent to which I would reveal my health information to this health website is" (Bansal et al., 2010)	unlikely/ likely	not probable/ probable	unwilling/ willing
"The extent to which I would reveal my financial/ health/personal information to this health/finance/ ecommerce website is" (Bansal et al., 2016)	unlikely/ likely	not probable/ probable	unwilling/ willing
"Please specify the extent to which you would reveal your personal information to this vendor." (Li et al., 2011)	unlikely/ likely	not probable/ probable	unwilling/ willing
"Given this hypothetical scenario, specify the extent to which you would reveal (the information) through the Internet." (Malhotra et al., 2004)	unlikely/ likely	not probable/ probable	willing/ unwilling*
"Please specify the extent to which you would reveal your personal information such as name, affiliation, job, educational background on Facebook" (Min & Kim, 2015)	unlikely/ likely	not probable/ probable	unwilling/ willing

Note. A mixture of seven-point (Li et al., 2011; Malhotra et al., 2004; Min & Kim, 2015) and eleven-point (Bansal et al., 2010, 2016) scales.
*One of the scales for Malhotra was reversed.

Table A6

Derived Codes and Breakouts

Code	Definition	References	Outcome- Group	Participants	Snippets	Representative Snippet
Behavior (BEHV)	An individual's likelihood to perform an action, prior demonstrated action, or prior stated action (conduct)	Bansal et al., 2010; Dinev & Hart, 2006; Dinev et al., 2008; Ku et al., 2013; Li, 2014; Li et al., 2017; Li et al., 2011; Li et al., 2015; Mao & Zhang, 2013; Min & Kim, 2015; Ozdemir et al., 2017; Schwaig et al., 2013; Son & Kim, 2008; Xu, 2010; Zhang et al., 2018	OG-A	2	4	"But uh I'm not intending to change anything. An like I said, I accept almost all requests for access and network." (11223476508, BEHV01)
			OG-H	3	7	"So I I toned that thing down. An I uh think I uh I uh may be doing the same with uh LinkedIn." (11224014306, BEHV03)
Benefit (BNFT)	An advantage or profit gained, value to the user	Dinev et al., 2013; Xu, Luo et al.,2011; Li et al., 1024	OG-A	3	5	"Uh, I uh I, I may be looking for another job soon. So, I am uh going to um hazard to keep the the line of communicaiton open, uh no changes, uh updating some of my uh um CV there and uh just you know um reaching out to people that I deem worthy uh in my um search for a a better job and or uh um to further further me in the job already have." (11188138618, BNFT01)
			OG-H	3	6	"I scrubbed it uh even before this couple of weeks, two three weeks ago uh with the intent of um ensuring um my network of IC and uh intel professionals recognize um the new duties and positions that I was that I'm currently in. And then more importantly, uh should I opt to uh leverage those that skill set into other arenas other commands? Um I had the requisite background that was uh verifiable um for potential recruiters and what." (11251351842, BNFT02)
Collection (COLL)	Any collection and processing of personal data, for purposes of influencing or managing those whose data have been garnered	Choi & Land, 2016	OG-A	3	4	"Uh, you know, the things that Facebook and I, I mean, it's just it's out there already and people have a a limited understanding of the totality of the knowledge that's uh available to a company like Facebook or to LinkedIn or to to others who have assembled these datasets and uh conducted analysis on them." (11223476508, COLL07)
			OG-H	3	8	"So uh I think I need some questions answered, um before I can move forward in having worked in the IC community for a short period of time, just a couple years, I know the capabilities of what they can do and and uh things they can look at." (11224014306, COLL05)

(continued)

Code	Definition	References	Outcome- Group	Participants	Snippets	Representative Snippet
Control (CNTL)	An individual's beliefs in his or her ability to manage the release and dissemination of personal information	Benson et al., 2015; Dinev et al., 2013; Kayhan & Davis, 2016; Schwaig et al. 2013; Xu, 2010; Xu et al., 2012; Xu, Dinev et al., 2011; Chen et al., 2013; Choi & Land, 2016; Li et al., 2014; Li et al., 2017	OG-A	3	20	"Okay. So once again, I mean it's, it's up to me to be careful of what I put out there in terms of uh you know what content I make available." (11269613365, CNTL12)
			OG-H	1	2	"And for that reason I don't have the only social media outlet I have is LinkedIn." (11205114603, CNTL14)
Errors (ERRS)	Deliberate or accidental inaccuracies	Mao & Zhang, 2013; Osatuyi, 2015; Smith et al., 1996; Stewart & Segars, 2002; Xu, 2010; Xu & Gupta, 2009; Xu et al., 2012; Zhang et al., 2013; Zhou, 2011	OG-A	0	0	Not Represented
			OG-H	1	4	"But uh, but for me, I have no need to be in that um in that world anymore. Uh, so as time goes on I, I remove a lot of those specific key terminologies simply because um that's in the past and it's no longer relevant." (11205114603, ERRS03)
General Privacy Concern (GPCN)	A user's general worry about personal information regarding its collection, storage, and usage (i.e., general privacy concern)	Kayhan & Davis, 2016; Li, 2014; Li et al., 2017; Li, Luo et al., 2011; Xu, Dinev et al., 2011	OG-A	2	4	"So, I, uh I value privacy." (11223476508, GPCN06)
			OG-H	3	5	"Um, I do value privacy." (11205114603, GPCN01)
Invasion (INVN)	An individual indicates current/past negative experience or outcome	Bansal et al., 2014; Bansal et al., 2016; Dinev et al., 2008; Li et al., 2014; Li & Unger, 2012; Xu, Luo et al., 2011	OG-A	0	0	Not Represented
			OG-H	2	7	"I've actually as an aside, I've had my identity stolen on Facebook, in one of these romance scam things and I had four to 500 uh fake profiles out there and people contacting me etc, which gave me great stress." (11224014306, INVN05)
Personality Traits (PNTR)	Characteristics that distinguish an individual (Big Five: extroversion, agreeableness, emotional instability, conscientiousness, intellect)	Bansal et al., 2010; Bansal et al., 2016; Chen, 2013a; Chen, 2013b; Chen & Sharma, 2015; Osatuyi, 2015	OG-A	0	0	Not Represented
			OG-H	1	2	"For me, I just don't find that myself that interesting to put so much information out there uh" (11205114603, PNTR01)

(continued)

Code	Definition	References	Outcome- Group	Participants	Snippets	Representative Snippet
Privacy Risk Belief (PRBF)	The expected loss potential associated with releasing personal information to a specific firm	Bansal et al., 2010; Chen, 2013a; Chen, 2013b; Chen & Sharma, 2015; Dinev & Hart, 2006; Dinev et al., 2013; Gerlach et al, 2015; Li, 2014; Li et al., 2010; Li et al., 2011; Li et al., 2014; Luo et al., 2013; Malhotra et al., 2004; Miltgen & Smith, 2015; Ozdemir et al., 2017; Treiblmaier & Chong, 2011; Xu, Dinev et al., 2011; Xu, Luo et al., 2011; Zhou, 2011; Zhou, 2015	OG-A	3	20	“But I think if you go out to social media sites, you gotta it's my position that you don't have any uh any expectation of privacy at that point." (11269613365, PRBF03)
			OG-H	2	5	“Uh, but, but for me, as soon as you put information out there, you, you lose control of it. So just a matter of risk you're willing to accept, accept that risk. Go for it." (11205114603, PRBF22)
Regulation (REGL)	A binding custom or practice of a community: a rule of conduct or action prescribed or formally recognized as binding or enforced by a controlling authority	Miltgen & Smith, 2015; Xu, 2010; Xu et al., 2012	OG-A	0	0	Not Represented
			OG-H	2	9	“Um and certainly looking through the uh amendments, probably the closest one that covers any sort uh of privacy information uh is both the 14th amendment uh or more importantly the Privacy Act of 1974 uh which in theory should prevent the unauthorized disclosure uh held by the government." (11251351842, REGL08)
Specific Privacy Concern (SPCN)	A user's worry about personal information regarding its collection, storage, and usage by a specific site or service	Bansal et al., 2010; Bansal et al., 2016; Benson et al., 2015; Li et al., 2011; Li, 2014; Luo et al., 2013; Mao & Zhang, 2013; Osatuyi, 2015; Wakefield, 2013; Xu et al., 2012; Zhang et al., 2013	OG-A	0	0	Not Represented
			OG-H	3	10	“So I do feel that uh, a little concerned about that based on what I know about Intel communities and sharing of information." (11224014306, SPCN07)
Usage (USGE)	Inappropriate/undisclosed application (e.g., discrimination and marketing) and sharing	Chen & Sharma, 2012; Chen & Sharma, 2015; Li & Unger, 2012; Mao & Zhang, 2014; Schwaig et al., 2013	OG-A	2	3	“And I believe that uh people generally generally are doing the right thing and abiding by the terms of service and uh and why they're using the system. But I know that that is not always the case." (11223476508, USGE06)
			OG-H	3	14	“Um, so, the uh uh or uh in addition, takes that information and uh puts it in in the public under a false light. Uh, and then lastly, uh uses my name and or uh my personal information for some sort of uh uh commercial advantage." (11251351842, USGE02)

Note. Snippet details provided after each in the following format: Participant ID, Code ID.

Table A7

Category/Code Distribution Analysis

	All Codes			Cat 1: Breach of Privacy		Cat 2: DTVP		Cat 3: SIPC		Cat 4: BITN		Cat 5: Supplementary	
	Categories	**Grp-Part**	**Grp-Snip**	**Part**	**Snip**	**Part**	**Snip**	**Part**	**Snip**	**Part**	**Snip**	**Part**	**Snip**
Categories	5	5	5	1	1	1	1	1	1	1	1	1	1
Codes	12*	24	24	24	24	24	24	24	24	24	24	24	24
Mean	9.200	1.875	5.792	24	1.208	0.917	1.417	0.667	1.667	0.792	1.125	0.542	0.875
Median	9.000	2.00	4.500	0.833	0.500	1.000	1.000	0.000	0.000	0.000	0.000	0.000	0.000
StdDev	1.304	1.191	5.618	0.500	1.865	0.923	1.718	0.963	1.786	1.062	1.541	0.779	1.484
Skewness	0.541	-0.582	1.414	0.963	2.391	0.887	1.756	1.392	1.526	1.165	1.172	1.054	1.627
Kurtosis	-1.488	-1.202	1.815	0.678	7.011	0.222	3.732	1.057	1.428	0.144	0.215	-0.430	1.113
D-value	0.248	0.249	0.182	-0.879	0.254	0.256	0.223	0.344	0.331	0.318	0.314	0.386	0.352
p-value	0.850	0.084	0.359	0.312	0.075	0.073	0.158	0.005	0.008	0.016	0.134	0.001	0.004
Normal?	yes	yes	yes	0.014	yes	yes	yes	no	no	no	no	no	no

Note. The * indicates the twelve codes were not broken out between the two groups.

Table A8

Category One, Breach of Privacy Breakout

Code	Outcome-Group	Participants	Snippets	Representative Snippet
Behavior (BEHV)	OG-A	0	0	Not presented.
	OG-H	1	1	“I'm torn on the subject. Um, after, after we, after we um engaged in our first um email conversation and exchange of information, I went back and looked at my stuff. And I think I made some adjustments and I'm still it's a constant, constant thing as, as uh life professional and personal changes, you you make adjustments to those public profiles you make, to adjust to those changes um for good or bad." (11205114603, BEHV06)
Benefit (BNFT)	OG-A	0	0	Not presented.
	OG-H	2	2	“I, I am on LinkedIn, which is an open site and I people use that to find resumes and things like that. Um, so in that respect, I'm fine uh, because I'm looking for something that's advantageous to me." (11224014306, BNFT06)
Collection (COLL)	OG-A	0	0	Not presented.
	OG-H	2	3	“But as time has gone by, and much more sophistication, on the ability to grab data from us all kinds of information." (11224014306, COLL03)
Control (CNTL)	OG-A	2	2	“Uh, I my resume is an assemblage of my life experience and I have not divulged any classified information. In fact, that resume was scrubbed and approved for release prior to it being posted anywhere or used for my job search." (11223476508, CNTL17)
	OG-H	0	0	Not presented.
Errors (ERRS)	OG-A	0	0	Not presented.
	OG-H	0	0	Not presented.
General Privacy Concern (GPCN)	OG-A	1	1	“So I post information on the internet with no expectation of privacy." (11223476508, GPCN04)
	OG-H	1	1	“Um, obviously, I'm not any celebrity or public figure who could reasonably assume to be recognized in the public and not be protected. But I would go on to say um that As a nonpublic individual, I uh certainly have the right to be protected from any intrusion on my solitude and my private affairs." (11251351842, GPCN08)

(continued)

Code	Outcome-Group	Participants	Snippets	Representative Snippet
Invasion (INVN)	OG-A	0	0	Not presented.
	OG-H	2	4	“I've been hacked and lost a lot of money about five or six years ago, and I thought I think it was from the Chinese, ah based on some, some uh research I did." (11224014306, INVN06)
Personality Traits (PNTR)	OG-A	0	0	Not presented.
	OG-H	0	0	Not presented.
Privacy Risk Belief (PRBF)	OG-A	3	8	“But I think if you go out to social media sites, you gotta it's my position that you don't have any uh any expectation of privacy at that point." (11269613365, PRBF03)
	OG-H	1	1	“Uh, so while while it's not a privacy issue, because you're volunteering to put your stuff out there, it's an argument could be made, it's in the public domain." (11205114603, PRBF06)
Regulation (REGL)	OG-A	0	0	Not presented.
	OG-H	1	1	“So I've submitted this particular instance, they do not have have just cause and and rather um the privacy that's being invaded, I would have, if you will, the essence uh or legal liability or legal uh ability to bring a lawsuit if damages or for damages that were incurred." (11251351842, REGL03)
Specific Privacy Concern (SPCN)	OG-A	0	0	Not presented.
	OG-H	2	2	“So I do feel that uh, a little concerned about that based on what I know about Intel communities and sharing of information." (11224014306, SPCN07)
Usage (USGE)	OG-A	0	0	Not presented.
	OG-H	2	3	“Uh, and then anybody that takes those, that data and disclose them in it with the intent to embarrass me or somehow discredit me with that private information causes us concern." (11251351842, USGE07)

Note. Snippet details provided after each in the following format: Participant ID, Code ID.

Table A9

Categories Three thru Four Breakouts

		Category 2: DTVP		Category 3: SIPC		Category 4: BITN	
Code	Outcome-Group	Participants	Snippets	Participants	Snippets	Participants	Snippets
Behavior (BEHV)	OG-A	0	0	0	0	2	4
	OG-H	0	0	1	1	3	5
Benefit (BNFT)	OG-A	1	1	0	0	3	3
	OG-H	1	1	0	0	3	3
Collection (COLL)	OG-A	0	0	2	3	0	0
	OG-H	1	1	1	2	1	1
Control (CNTL)	OG-A	3	7	1	4	1	3
	OG-H	1	2	0	0	0	0
Errors (ERRS)	OG-A	0	0	0	0	0	0
	OG-H	1	1	1	1	1	1
General Privacy Concern (GPCN)	OG-A	1	2	0	0	1	1
	OG-H	3	4	0	0	0	0
Invasion (INVN)	OG-A	0	0	0	0	0	0
	OG-H	1	1	0	0	1	1
Personality Traits (PNTR)	OG-A	0	0	0	0	0	0
	OG-H	1	2	0	0	0	0
Privacy Risk Belief (PRBF)	OG-A	1	2	2	3	1	3
	OG-H	2	4	0	0	0	0
Regulation (REGL)	OG-A	0	0	0	0	0	0
	OG-H	2	2	1	2	0	0
Specific Privacy Concern (SPCN)	OG-A	0	0	0	0	0	0
	OG-H	2	3	3	5	0	0
Usage (USGE)	OG-A	0	0	1	1	2	2
	OG-H	1	1	3	6	0	0

Note. Associated representative snippets were provided in Table 14.

Table A10

Category Five, Supplementary Breakout

Code	Outcome-Group	Participants	Snippets	Representative Snippet
Behavior (BEHV)	OG-A	0	0	Not presented.
	OG-H	0	0	Not presented.
Benefit (BNFT)	OG-A	1	1	“So I'm not there's not a lot of hiding unless I go, you know, off grid and I'm not willing to do that, the benefit is worth the uh um uh the effort." (11188138618, BNFT07)
	OG-H	0	0	Not presented.
Collection (COLL)	OG-A	1	1	“Uh um there is a way that they could probably figure out my birthday. But you know, again, there's so much public knowledge out there that for a few dollars at a time, you could put together a fairly decent um uh biography of [NAME REMOVED]." (11188138618, COLL01)
	OG-H	1	1	“I think as we're moving forward and gaining more capabilities in our and an the ways that we're able to collect and store data" (11224014306, COLL06)
Control (CNTL)	OG-A	2	4	“So people have to take a personal uh position on what they're doing, what they're posting out there." (11269613365, CNTL04)
	OG-H	0	0	Not presented.
Errors (ERRS)	OG-A	0	0	Not presented.
	OG-H	1	1	“So this is for me this is a good reminder to go back in there and double check on things to make sure that uh the image that I'm trying to present is a s professional and uh accurate as possible." (11205114603, ERRS04)
General Privacy Concern (GPCN)	OG-A	0	0	Not presented.
	OG-H	0	0	Not presented.
Invasion (INVN)	OG-A	0	0	Not presented.
	OG-H	1	1	“And I want to cut back on some of this other stuff. Uh, especially as I get older, I don't want to be losing a nickel to anybody who uh may steal my stuff. I lost 25 thousand dollars a few years ago, though, was FDIC a little bit of a ramble there." (11224014306, INVN04)

(continued)

Code	Outcome-Group	Participants	Snippets	Representative Snippet
Personality Traits (PNTR)	OG-A	0	0	Not presented.
	OG-H	0	0	Not presented.
Privacy Risk Belief (PRBF)	OG-A	2	4	“So it's a social media site. So anyway, and I know there's a lot, a lot of millennials, I guess there's an expectation of these things to be more than what they were intended to be, I think, so. These expectations evolve. And I don't really know what the foundation for it is why they believe that." (11269613365, PRBF09)
	OG-H	0	0	Not presented.
Regulation (REGL)	OG-A	0	0	Not presented.
	OG-H	2	4	“But, um, I think we need to relook things and starting with many of the laws that are in place and the ability to collect on on Americans, and then also the ability for private companies to collect on us also." (11224014306, REGL04)
Specific Privacy Concern (SPCN)	OG-A	0	0	Not presented.
	OG-H	0	0	Not presented.
Usage (USGE)	OG-A	0	0	Not presented.
	OG-H	2	4	“The probably in in in stepping back it uh this is not the first time that uh an entity agency has looked to scrape and or um use this information for, you know, malicious type attacks." (11251351842, USGE14)

Note. Snippet details provided after each in the following format: Participant ID, Code ID.

Appendix B

Questionnaire

DTVP was measured using three items, SIPC was measured using four items, and BITN was measured using three items. All constructs were measured with a seven-point scale ranging from 1 to 7. A single item each measured both demographic factors (age and sex). Finally, as the potential existed for participants to modify their LinkedIn profile before contact, one additional binary scale question (suitability) was included as a participant disqualifier.

Table B1

Questionnaire

Questionnaire

Participant Letter for Anonymous Surveys
NSU Consent to be in a Research Study Entitled

The Influence of an Individual's Disposition to Value Privacy
in a Non-Contrived Study

Introduction

A website called ICWATCH (https://icwatch.wikileaks.org/) uses scraped LinkedIn data to identify members of the Intelligence Community and collate them into a searchable database. Your LinkedIn profile was scraped and stored in ICWATCH. As a LinkedIn connection of yours, and as the focus of my Ph.D. dissertation, I would like to understand better if you believe this to be a privacy concern and if so, will you take action on LinkedIn to mitigate this. I hope that you will participate in a short questionnaire (15 questions) and ideally, in a subsequent interview about the situation.

(continued)

The specific participant consent details should be read here Research Participant Consent Letter

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

If you have read the above information and voluntarily wish to participate in this research study, please select the consent option below.

Consent (binary: I consent/I decline)	
	Do you understand and do you want to be in the study? If you have read the above information and voluntarily wish to participate in this research study, please select the consent option below.
Control variables (one ordinal: range, one binary: 0/1); age stratification modeled from reference studies (Min & Kim, 2015; Zhang et al., 2018)	
Age	< 20, 20-29, 30-39, 40-49, 50+
Sex	Female, Male
Suitability (binary: yes/no)	
	Is any part of your LinkedIn profile publicly visible (e.g., any part of your LinkedIn profile can be found using a search engine such as Google or Bing)?
DTVP Seven-point scales anchored with “strongly disagree” and “strongly agree”	
DTVP1	Compared to others, I am more sensitive about the way online companies handle my personal information.
DTVP2	To me, it is most important to keep my privacy intact from online companies.
DTVP3	I am concerned about threats to my personal privacy today.
Situational Privacy Concerns Seven-point scales anchored with “strongly disagree” and “strongly agree”	
SIPC1	I am concerned that the information I submit on LinkedIn could be misused.
SIPC2	I am concerned that a person can find private information about me from LinkedIn.
SIPC3	I am concerned about submitting information on LinkedIn because of what others might do with it.

(continued)

SIPC4	I am concerned about submitting information on LinkedIn because it could be used in a way I did not foresee.
Behavioral Intention Seven-point scales anchored with “strongly disagree” and “strongly agree.” *Question:* Please specify the extent to which you would continue to share your LinkedIn profile publicly, exposing profile data to ICWATCH.	
BITN1	Unlikely/likely
BITN2	Not probably/probable
BITN3	Unwilling/willing
Interview (one binary: yes/no, one participant submission: email)	
INTV1	Are you willing to be interviewed about this situation?
INTV2	My email address for scheduling a future interview is __________

Appendix C

Raw Survey Results

Table C1

Raw Survey Results

ID	Consent	Qualifier	Age	Sex	Disposition to Value Privacy			Situation-Specific Privacy Concern				Behavioral Intention			Interview
					DTVP1	DTVP2	DTVP3	SIPC1	SIPC2	SIPC3	SIPC4	BITN1	BITN2	BITN3	
11859463589	1	1	3	2	7	5	6	4	3	3	5	7	7	7	1
11652267559	1	1	5	2	6	4	6	5	5	5	5	6	6	5	2
11630105120	1	1	4	1	1	1	3	1	1	1	1	7	7	7	1
11565649049	1	1	5	2	5	5	5	5	5	5	5	6	6	6	1
11448408267	1	1	5	2	6	6	6	6	6	6	6	3	3	3	2
11445999311	1	1	5	2	6	5	6	6	3	5	6	5	5	5	2
11431880759	1	1	4	2	5	5	7	4	5	5	6	6	6	4	2
11430743638	1	1	4	2	6	6	6	4	4	3	4	4	4	4	1
11424945022	1	1	5	2	6	7	5	7	7	6	7	5	5	2	1
11423552387	1	1	3	2	6	6	7	4	5	4	4	2	3	1	1
11420589586	1	1	4	2	6	6	7	6	5	4	6	5	4	3	1
11420277538	1	1	4	1	4	4	4	4	4	6	6	4	4	4	1
11420005672	1	1	5	2	4	4	4	4	4	4	4	4	4	4	1
11388874236	1	1	5	1	6	7	6	4	4	5	7	6	6	4	2
11336653975	1	1	5	2	7	7	6	5	5	4	4	5	6	5	2
11292890157	1	1	4	2	6	4	5	5	3	5	5	5	5	4	2
11292806106	1	1	3	2	6	6	6	7	6	6	6	3	3	2	1
11283971091	1	1	5	2	7	7	7	7	7	7	7	3	3	2	2

(continued)

ID	Consent	Qualifier	Age	Sex	Disposition to Value Privacy			Situation-Specific Privacy Concern				Behavioral Intention			Interview
					DTVP1	DTVP2	DTVP3	SIPC1	SIPC2	SIPC3	SIPC4	BITN1	BITN2	BITN3	
11270499000	1	1	5	2	6	6	5	4	4	4	4	5	6	5	2
11269613365	1	1	5	2	1	1	1	1	1	1	1	7	7	7	1
11269116413	1	1	5	2	6	7	7	5	1	1	1	7	7	7	1
11269077529	1	1	5	2	6	6	7	5	3	5	5	5	5	5	1
11262237459	1	1	4	1	6	5	4	5	2	4	4	6	6	5	1
11258534181	1	1	5	2	7	6	6	5	4	4	5	3	3	2	1
11258094277	1	1	5	2	6	6	2	5	5	5	6	6	6	5	1
11254816449	1	1	3	2	4	6	7	6	5	5	6	5	5	5	1
11254766819	1	1	3	2	6	6	6	5	5	5	5	5	3	5	1
11253964035	1	1	4	2	7	7	7	6	5	3	3	5	5	5	1
11252427362	1	1	5	2	6	6	6	6	6	6	6	2	2	2	2
11251682995	1	1	2	1	3	6	5	3	2	3	4	2	2	2	1
11251597916	1	1	5	2	6	6	7	6	5	4	4	5	5	5	1
11251351842	1	1	5	2	7	7	7	7	7	7	7	3	3	3	1
11250719712	1	1	4	2	6	6	7	6	5	5	5	6	6	6	2
11250710475	1	1	5	2	6	7	6	6	6	5	5	3	5	5	2
11248992091	1	1	5	2	4	5	5	3	1	3	3	7	7	7	1
11248576429	1	1	5	2	5	6	6	4	3	3	3	6	6	4	1
11246837913	1	1	5	2	7	6	6	5	5	5	6	7	7	6	1
11242439726	1	1	3	2	6	5	6	6	3	4	6	3	5	4	2
11240433307	1	1	3	2	7	7	7	7	7	7	7	6	6	4	1
11240361396	1	1	5	2	5	5	7	6	6	5	6	6	6	6	1
11240246323	1	1	3	1	5	5	5	3	3	2	2	5	5	5	1
11240219945	1	1	5	2	5	6	7	4	4	4	3	6	5	6	1
11240201867	1	1	5	2	4	6	7	4	7	4	7	6	4	6	1
11239357735	1	1	4	2	6	5	5	7	6	6	7	5	5	5	2
11239279776	1	1	4	2	3	3	2	4	1	2	2	6	6	6	2
11239144520	1	1	4	2	3	5	5	5	3	3	5	6	6	6	2
11238329302	1	1	5	2	7	7	7	6	4	4	6	5	5	5	1
11238118996	1	1	4	1	6	5	1	5	6	3	4	7	5	3	1
11237599422	1	1	5	2	3	3	3	5	3	3	5	5	5	5	1
11227298696	1	1	5	2	4	4	5	4	4	4	3	6	6	6	2
11227117168	1	1	4	2	7	7	7	7	7	7	7	5	5	3	2
11226351367	1	1	5	2	7	7	7	7	5	5	5	7	7	6	1
11224014306	1	1	5	2	7	7	7	7	7	7	7	4	4	4	1
11223795290	1	1	5	2	4	4	4	4	4	4	4	4	4	4	2

(continued)

ID	Consent	Qualifier	Age	Sex	Disposition to Value Privacy			Situation-Specific Privacy Concern				Behavioral Intention			Interview
					DTVP1	DTVP2	DTVP3	SIPC1	SIPC2	SIPC3	SIPC4	BITN1	BITN2	BITN3	
11223476508	1	1	5	2	2	2	2	2	1	1	1	7	7	7	1
11218350809	1	1	5	2	6	5	7	5	5	4	4	7	7	7	1
11211977877	1	1	4	2	5	5	5	1	1	1	1	7	7	7	2
11208486428	1	1	5	2	5	6	6	5	5	5	5	6	6	6	1
11206905505	1	1	3	2	5	5	5	4	4	4	5	5	5	5	1
11206505729	1	1	5	1	4	5	5	5	5	5	6	5	5	5	2
11205114603	1	1	5	2	7	7	7	7	6	6	6	3	3	3	1
11205018115	1	1	5	2	1	4	4	5	4	4	5	7	7	7	1
11192764538	1	1	5	2	4	6	4	5	5	4	5	4	4	4	1
11188138618	1	1	5	2	2	2	2	2	2	2	2	6	6	6	1
11186388785	1	1	4	2	6	6	6	6	5	5	5	6	6	6	1

Appendix D

Snippet-Coding

Table D1

Total Snippets by Topic and Coding

Topic	Code	OG	Snippet
Topic One, "For the next few minutes, let's discuss if this is a breach of privacy."	BEHV	A	Not Represented
		H	"I'm torn on the subject. Um, after, after we, after we um engaged in our first um email conversation and exchange of information, I went back and looked at my stuff. And I think I made some adjustments and I'm still it's a constant, constant thing as, as uh life professional and personal changes, you you make adjustments to those public profiles you make, to adjust to those changes um for good or bad." (11205114603, BEHV06, 3)
	BNFT	A	Not Represented
		H	"I, I am on LinkedIn, which is an open site and I people use that to find resumes and things like that. Um, so in that respect, I'm fine uh, because I'm looking for something that's advantageous to me." (11224014306, BNFT06, 3) "Uh, on the one hand, people people put all sorts of stuff on their profiles um, in the effort to either get seen, get approached for work, establish a professional network or any number of things." (11205114603, BNFT10, 3)

(continued)

Topic	Code	OG	Snippet
Topic One, "For the next few minutes, let's discuss if this is a breach of privacy." (continued)	COLL	A	Not Represented
		H	"But as time has gone by, and much more sophistication, on the ability to grab data from us all kinds of information." (11224014306, COLL03, 3) "On the other hand, if you're not aware that your stuff is getting scooped up like that, maybe it's an issue for some um frankly." (11205114603, COLL14, 3) "On the other hand, uh, I'm not sure many people realize that whatever they put out there is being um scooped up by whatever um artificial uh aggregators for lack of a better word, um to assist uh whatever agency creates those aggregators." (11205114603, COLL15, S)
	CNTL	A	"I think I told you that my questionnaire I think that, you know, you could have as much as an individual, I could have as much privacy as I want." (11269613365, CNTL13, 3) "Uh, I my resume is an assemblage of my life experience and I have not divulged any classified information. In fact, that resume was scrubbed and approved for release prior to it being posted anywhere or used for my job search." (11223476508, CNTL17, 2)
		H	Not Represented
	GPCN	A	"So I post information on the internet with no expectation of privacy" (11223476508, GPCN04, 2.5)
		H	"Um, obviously, I'm not any celebrity or public figure who could reasonably assume to be recognized in the public and not be protected. But I would go on to say um that As a nonpublic individual, I uh certainly have the right to be protected from any intrusion on my solitude and my private affairs." (11251351842, GPCN08, 3)
	INVN	A	Not Represented
		H	"Yes um yes and no, I'm sorry, I've have to answer it that way." (11224014306, INVN01, 3) "So, the um the breaches the breach of privacy is actually an intrusion into the personal life of another specifically without just cause." (11251351842, INVN02, 3) "So, so the breach of privacy is not fully satisfied, if you will, under under this particular uh situation. Under this particular topic, ie a breach of privacy, that they scraped my personally available information um that anybody with a reasonable uh basis could do you know, from uh Facebook, um and that is made to the general public, certainly. Uh, but does that necessarily constitute a breach of my privacy? Uh, no, not at this point." (11251351842, INVN03, 3) "I've been hacked and lost a lot of money about five or six years ago, and I thought I think it was from the Chinese, ah based on some, some uh research I did." (11224014306, INVN06, 3)

(continued)

Topic	Code	OG	Snippet
Topic One, "For the next few minutes, let's discuss if this is a breach of privacy." (continued)	PRBF	A	"Although they try to do it. I mean, it's just, I mean, I don't know how hard it would be to for their platform to work with uh personalized privacy settings. So I really don't expect, I have no expectation of privacy on that stuff." (11269613365, PRBF02, 3) "But I think if you go out to social media sites, you gotta it's my position that you don't have any uh any expectation of privacy at that point" (11269613365, PRBF03, 3) "There was never any expectation on my part that that information would be considered private or protected in any way." (11223476508, PRBF04, 3) "No, cuz uh and and the reason why I believe that is when you join LinkedIn, you give up inherent rights to privacy by stepping into LinkedIn." (11188138618, PRBF07, 3) "And so I was fully aware that both LinkedIn would use my information, as well as the availability of that information to others uh uh or whoever scraped or used or viewed that information." (11223476508, PRBF08, 3) "I just want to let you know, I can elaborate if you want more, but I just know that that's how I feel it just uh. You know, just by the term social media. So LinkedIn, Facebook, Twitter, all those are uh social media sites, and I have no expectation of privacy on any of those sites." (11269613365, PRBF10, 3) "So, I mean, that's why they're called social media, right? So uh I guess that pretty much answers my the question." (11269613365, PRBF18, 3) "I fully am aware that the information that I post to any public page is available to any person." (11223476508, PRBF21, 3)
		H	"Uh, so while while it's not a privacy issue, because you're volunteering to put your stuff out there, it's an argument could be made, it's in the public domain." (11205114603, PRBF06, 2)
	REGL	A	Not Represented
		H	"So I've submitted this particular instance, they do not have have just cause and and rather um the privacy that's being invaded, I would have, if you will, the essence uh or legal liability or legal uh ability to bring a lawsuit if damages or for damages that were incurred." (11251351842, REGL03, 2)
	SPCN	A	Not Represented
		H	"Um, so, for me it's it's a double edged sword it could be construed as a privacy issue. While on the other hand, it might not be depending on on um the the exact nature of one your understand you as an individual your understanding of what those profiles are and are used for and two, the information you're putting out there." (11205114603, SPCN02, 3) "So I do feel that uh, a little concerned about that based on what I know about Intel communities and sharing of information." (11224014306, SPCN07, 3)

(continued))

Topic	Code	OG	Snippet
Topic One, "For the next few minutes, let's discuss if this is a breach of privacy." (continued)	USGE	A	Not Represented
		H	"Um, so, the uh uh or uh in addition, takes that information and uh puts it in in the public under a false light. Uh, and then lastly, uh uses my name and or uh my personal information for some sort of uh uh commercial advantage." (11251351842, USGE02, 2.5) "Uh, and then anybody that takes those, that data and disclose them in it with the intent to embarrass me or somehow discredit me with that private informatioin causes us concern." (11251351842, USGE07, 3) "But I don't know what's going on on this site where my information is going." (11224014306, USGE13, 2.5)
Topic Two, "For the next few minutes, let's discuss your disposition to value privacy." (continued)	BNFT	A	"So it's, it's stuff that I wouldn't mind put it on there because I want a large number of people to be able to see it, i.e., my friends, so I'm not looking for any real privacy in those settings." (11269613365, BNFT09, 3)
		H	"And I established that for a specific reason. Which has evolved over time." (11205114603, BNFT03, 3)
	COLL	A	Not Represented
		H	"I, I suspect the bigger the bigger issue and bigger concern um would be to take uh the information from the OPM or some of the other databases that have been breached and and kind of uh meld them together if you will." (11251351842, COLL09, 3)
	CNTL	A	"So if if I don't want uh, if if I want to be private, that I don't engage, that's that's the only way to be completely private." (11188138618, CNTL02, 3) "So I feel I'm in control that. So uh if I want something to be private, then I won't put it on a social media site. So I mean, there's things that you look at my social media sites, I probably, I'm guessing you probably have. There's not much out there. So it's, uh, it's pretty vanilla. And like, I try to stay away from politics or a lot of personal opinions. Most of it has to do with pictures of the family and stuff like that" (11269613365, CNTL10, 3) "I take steps to ensure that what I post or provide to others is information that I intend to provide that, that I've thought about the implications of that information and the, the uh, you know, the receiver of that information and and uh those sorts of contingencies or outcomes." (11223476508, CNTL15, 2) "If I want privacy, then I don't engage that's the only way to secure absolute privacy." (11188138618, CNTL16, 3) "I, I do not post a lot of social media information." (11223476508, CNTL18, 3) "I have a Twitter account, but I don't tweet you know, I mean, I um so, I don't, I don't provide a lot of information, because I consider much of that private." (11223476508, CNTL19, 3) "If I'm looking for privacy, then I'll send you know, a personal email or letter, write someone a letter and send it." (11269613365, CNTL22, 3)
		H	"Um, I don't, I don't care to put much information out about myself. That's just my nature." (11205114603, CNTL01, 3) "And for that reason I don't have the only social media outlet I have is LinkedIn." (11205114603, CNTL14, 3)

(continued)

Topic	Code	OG	Snippet
Topic Two, "For the next few minutes, let's discuss your disposition to value privacy." (continued)	ERRS	A	Not Represented
		H	"Professional reasons I had to and uh but every now and then I go back in there and I make some adjustments, make some updates, take some stuff off that are no longer relevant." (11205114603, ERRS01, 3)
	GPCN	A A	"So that so I consider myself a very private person in that regard in that." (11223476508, GPCN05, 3) "So, I, uh I value privacy." (11223476508, GPCN06, 2.5)
		H	"Um, I do value privacy." (11205114603, GPCN01, 3) "So, ah right now, at this point, I'm very concerned about my privacy." (11224014306, GPCN02, 3) "I don't feel the need to share my life with strangers." (11205114603, GPCN07, 2.5) "Uh, at the end of the day, I certainly value the right to be left alone." (11251351842, GPCN09, S)
	INVN	A	Not Represented
		H	"I was ah hacked through the OPM hack a couple of years ago, and God knows who has my Social Security numbers and things like that." (11224014306, INVN07, S)
	PNTR	A	Not Represented
		H	"For me, I just don't find that myself that interesting to put so much information out there uh." (11205114603, PNTR01, 2.5) "I'm not a very uh outgoing or extroverted person," (11205114603, PNTR02, S)

(continued)

Topic	Code	OG	Snippet
Topic Two, "For the next few minutes, let's discuss your disposition to value privacy." (continued)	PRBF	A	"Um so uh I don't um believe that knowing my name, and uh, and uh knowing my disposition, but through conversation, either over the phone or uh, or in person is anything more than just um that person that I'm engaging with, using their uh, their skills and their uh techniques of a, of a um observation to to make a make a deduction." (11188138618, PRBF20, 3) "And uh so um when I say that, you know, I'm gonna engage somebody um through a conversation, I'm willing, uh at that point I made a decision that I'm gonna give up some of my property to go uh um further. " (11188138618, PRBF25, S)
		H	"Um, with that said, I do realize that uh let's let's put it this way, the, my philosophy is um, if you don't want people to know something, don't put it on the internet." (11205114603, PRBF05, 3) "Because once it's out there, you lose complete control over it. It's no longer yours. you're you're you're on someone else's platform, therefore, it's at least partially theirs and they can do with it. What they want. If you're okay with that, then the rules governing privacy are a little bit looser. Uh, if you're not okay with that, don't use a platform. " (11205114603, PRBF16, 3) "Uh my personally identifiable information is uh um thought to be at least protected from public scrutiny, especially as a employee of the government, uh but I think uh recent breaches with, especially with the Office of Personnel Management has almost made that null and void." (11251351842, PRBF17, 3) "Uh, but, but for me, as soon as you put information out there, you, you lose control of it. So just a matter of risk you're willing to accept, accept that risk. Go for it." (11205114603, PRBF22, 3)
	REGL	A	Not Represented
		H	"And actually was a little disappointed when the Patriot Act was ah, I think if I'm not mistaken, I know it's being re-looked, I think it may have been approved, but I'm not sure we've made any adjustments on that. For our, our, our new um for this period, any updates, if you will, excuse me." (11224014306, REGL05, 3) "Um and certainly looking through the uh amendments, probably the closest one that covers any sort uh of privacy information uh is both the 14th amendment uh or more importantly the Privacy Act of 1974 uh which in theory should prevent the unauthorized disclosure uh held by the government." (11251351842, REGL08, 2.5)
	SPCN	A	Not Represented
		H	"I never have been that way, whether before the internet or even even today, so it's not really uh, for me, it's not really a privacy specific issue. It's more of a personality and I guess the nature of me issue." (11205114603, SPCN05, 3) "I become quite concerned, also concerned with little funny things that happen when ah I'm standing around talking about a subject and it shows up on my ah Amazon feed or something of that nature." (11224014306, SPCN08, 3) "So yes, I'm concerned." (11224014306, SPCN09, 3)

(continued)

Topic	Code	OG	Snippet
Topic Two, "For the next few minutes, let's discuss your disposition to value privacy." (continued)	USGE	A	Not Represented
		H	"So ah somebody's grabbing my information, ah somebody's using it for whether it's sales, or whether to rob me or use my uh uh social security number." (11224014306, USGE12, 3)
Topic Three, "For the next few minutes, let's discuss your level of concern regarding LinkedIn scraping/posting your data."	BEHV	A	Not Represented
		H	"And I think I went back there and uh did a general scrub and use more general terminology, because I'm not I'm no longer in that in that profession." (11205114603, BEHV02, 3)
	COLL	A	"Uh, you know, the things that Facebook and I, I mean, it's just it's out there already and people have a a limited understanding of the totality of the knowledge that's uh available to a company like Facebook or to LinkedIn or to to others who have assembled these datasets and uh conducted analysis on them." (11223476508, COLL07, 2.5) "But it does uh provide a central repository for somebody who's interested and desires to have introspection into the US intelligence community. Um, your thesis statement talks about, um you know, code words and different information and the assembly of aggregate information and, and I, I believe that that is an issue in uh general that the, you know, a lot can be learned from uh, from assembling different data sources and analyzing those. And um so, at some point, you know, we are as a, as a human race going to really have to come to grips with the understanding of what privacy is because because of the potential for these different data sets to be assembled." (11223476508, COLL12, 3) "So I thought, I thought that was it I just wasn't real sure ICWATCH almost sounds like a government function so but I'm sure the government does the same thing with my with me too also so same thing ICWATCH. I'm guessing the government's also doing the same thing." (11269613365, COLL13, 3)
		H	"So uh I think I need some questions answered, um before I can move forward in having worked in the IC community for a short period of time, just a couple years, I know the capabilities of what they can do and and uh things they can look at." (11224014306, COLL05, 3) "Uh, it does bother me because I don't know what they're doing with I know what the NSA programs are with phones and things like that of gathering data uh and and uh holding on to it, but only looking specifically when they need something. Um, I don't feel comfortable with somebody holding on to uh critical information about me, what are they using it for? What are they scraping it for? And what are they doing with it?" (11224014306, COLL11, 2.5)

(continued)

Topic	Code	OG	Snippet
Topic Three, "For the next few minutes, let's discuss your level of concern regarding LinkedIn scraping/posting your data." (continued)	CNTL	A	"So once again, I thought, you know if your personal responsibility to montior that, so I wouldn't expect uh uh a site, a social media site to be able to uh protect, I shouldn't be discussing that." (11269613365, CNTL07, 3)
			"I mean, I have a resume that's been there forever, and it's pretty vanilla. And the government's seen it. So it's uh, you know, once again, I'm kind of careful about that. I don't go any further than that." (11269613365, CNTL09, 3)
			"Okay. So once again, I mean it's, it's up to me to be careful of what I put out there in terms of uh you know what content I make available." (11269613365, CNTL12, 3)
			"So we want to talk about additional data that I make sure that we talk in a space somewhere where I know that it's, it's uh been SCIF'd for the discussion that we're about to have." (11269613365, CNTL20, 3)
		H	Not Represented
	ERRS	A	Not Represented
		H	"But uh, but for me, I have no need to be in that um in that world anymore. Uh, so as time goes on I, I remove a lot of those specific key terminologies simply because um that's in the past and it's no longer relevant." (11205114603, ERRS03, 2)
	PRBF	A	"So, you know, again uh, you know, I made the conscious effort, uh the conscious decision that that what they were going to be able to ascertain from me was uh not going to directly uh um affect me and uh in a negative way and and not to negatively uh affect me in an indirect ways either. Um I don't think that a uh bad actor could um necessarily get enough information to do do me or my um family harm." (11188138618, PRBF14, 3)
			"So maybe you have a question about it, you know, we've been instructed to contact the government, if you have, if you have any concerns, so uh most of that stuff has been vetted that that I would ever talk about, I have very little out there." (11269613365, PRBF15, 3)
			"Uh, again, you know I uh my concern is a, is really kind of moot um as I engage in those already um when uh when I decided to go onto LinkedIn, you know, I I knew um that uh there was going to be a um uh the disability because I I knew of this ability to scrape information and and uh um you to fit into algorithms that would be able to uh ascertain my likes, dislikes, and and basically pull the strings, my personality." (11188138618, PRBF19, 2)
		H	Not Represented
	REGL	A	Not Represented
		H	"Um um but but looking at the some of the previous models, um especially with uh Chelsea Manning, and and uh and others. Um it it certainly did harmful and uh severe damage to the US government writ large." (11251351842, REGL01, 3)
			"Um, so um you know, the the fact that ICWATCH has violated personal privacy in the past it has and and and, more importantly, the US government's resolve to do anything about it. Um um you know, has has me equally concerned and I say that because uh uh Julian Assange uh has been uh under um has not been brought to trial in 10 years despite being uh currently at trial as we speak." (11251351842, REGL07, 3)

(continued)

Topic	Code	OG	Snippet
Topic Three, "For the next few minutes, let's discuss your level of concern regarding LinkedIn scraping/posting your data." (continued)	SPCN	A	Not Represented
		H	"Um, on the other hand, it was it was the more I thought about it, the more I realized, well, that's to be expected." (11205114603, SPCN01, 3) "It does bother me, when I first saw it, I was concerned." (11224014306, SPCN03, 2) "Okay, yeah, that was a surprise to me. Um, I, at first I was I was uh, I was quite unhappy about that. But on the other end, I went back to my original philosophy. Well, I put the stuff out there." (11205114603, SPCN04, 3) "And it makes me concerned. I just don't, uh I just don't gave enough information about it." (11224014306, SPCN06, 3) "Um, surely, uh ICWATCH um their behavior certainly raises red flags." (11251351842, SPCN10, S)
	USGE	A	"Uh I believe that IC I don't know where ICWATCH is located or the people that are involved in it, but they potentially make it easy for enemies of the United States to assemble information. " (11223476508, USGE09, 2)
		H	"Um but uh you know, his his model of behavior, not only with ICWATCH, but similar programs were designed to do that bring discredit on um the folks in that community. So it does raise a red flag. They could certainly be used um with a nefarious attack." (11251351842, USGE01, 3) "Well uh, what are they doing with it?" (11224014306, USGE05, 3) "So I guess my question, you know, if I'd summed up in one statement, what are you doing with it?" (11224014306, USGE08, 3) "Uh, for whatever purposes um, you know, could be nefarious, it could simply be trying to find the right people for the right position across the IC uh or other other agencies, private and public." (11205114603, USGE10, 3) "Um, using the WikiLeaks model as a conduit to the general public, um um it was in my mind anyways that that uh that breach that scraping of information that technique that model is uh designed more clear or clearly more designed, if you will, to harm the IC community and and writ large the US government." (11251351842, USGE11, 3) "Um and at the end of the day, the question comes into uh what the intent is, um you know, is the intent malicious Um, that's questionable." (11251351842, USGE16, S)

(continued)

Topic	Code	OG	Snippet
Topic Four, "Finally, let's discuss your intention to modify your LinkedIn profile's visibility."	BEHV	A	"But uh I'm not intending to change anything. An like I said, I accept almost all requests for access and network." (11223476508, BEHV01, 3)
			"So, you know, I'm not I'm not um anticipating any change." (11188138618, BEHV04, 2.5)
			"I don't I don't have plans right now." (11188138618, BEHV08, 3)
			"Uh, I do not intend to change anything. I update my resume periodically. I don't intend to change any settings." (11223476508, BEHV11, S)
		H	"So I I toned that thing down. An I uh think I uh I uh may be doing the same with uh LinkedIn." (11224014306, BEHV03, 3)
			"Yeah, that's funny you bring that up. Uh, aside from this, I was, someone had mentioned something like this just the other day I forget the specific, but um I, I, I thought I was in a private mode, I'm going to have to take another look, not just with my LinkedIn, but also with Facebook and a few other things." (11224014306, BEHV05, 3)
			"Um, so quite honestly, I like it the way it is." (11251351842, BEHV07, 3)
			"Okay, yeah um. I plan on I don't do it as frequently as I should. But uh not, uh not because of you specifically, or the subject matter. But yeah, before the weekend. I'll probably go back in there and um take another look and see what, what not image but." (11205114603, BEHV09, 3)
			"I'm not going to be job hunting a lot more late in the next few years, but I, I think I'm going to take another look at it and see what is accessible. " (11224014306, BEHV10, 3)
	BNFT	A	"Uh, I uh I, I may be looking for another job soon. So, I am uh going to um hazard to keep the the line of communicaiton open, uh no changes, uh updating some of my uh um CV there and uh just you know um reaching out to people that I deem worthy uh in my um search for a a better job and or uh um to further further me in the job already have." (11188138618, BNFT01, 3)
			"I acccept nearly all requests to uh know whenever it's not a friend request that leaded at LinkedIn but but I think there's value in networking." (11223476508, BNFT05, 3)
			"So that to me is a social media site's all about us out there trying to basically generate a network." (11269613365, BNFT08, 2)
		H	"I scrubbed it uh even before this couple of weeks, two three weeks ago uh with the intent of um ensuring um my network of IC and uh intel professionals recognize um the new duties and positions that I was that I'm currently in. And then more importantly, uh should I opt to uh leverage those that skill set into other arenas other commands? Um I had the requisite background that was uh verifiable um for potential recruiters." (11251351842, BNFT02, 2.5)
			"What public profile of me I want out there to strengthen or expand my network. Take it in the direction I want it to go." (11205114603, BNFT04, 3)
			"I don't have a lot of information on there except of who I am, uh jobs I've held, which is advantageous to me." (11224014306, BNFT11, S)

(continued)

Topic	Code	OG	Snippet
Topic Four, "Finally, let's discuss your intention to modify your LinkedIn profile's visibility." (continued)	COLL	A	Not Represented
		H	"Um again, I don't know, they're we're looking at if they've taken everything, um IP addresses, any phone numbers that may or may not be in there. Anything, anything I may have said." (11224014306, COLL08, 2)
	CNTL	A	"So I don't I don't perceive any, any uh expectation of privacy when dealing with those sites but if I want to be private, then I'll write an email, I won't, it won't be on some kind of uh, I guess it's, you know, there's a push-pull arrangement, right? It won't be on a site where people can pull data." (11269613365, CNTL06, 2) "If I'm worried about it, it's gonna be a situation where I'll push it to the guy. And it won't be through the site, it'll be through an email or something a little bit more secure." (11269613365, CNTL11, 2.5) "I know everybody that's on my site." (11269613365, CNTL21, 3)
		H	Not Represented
	ERRS	A	Not Represented
		H	"Um, as I mentioned before, I'm definitely uh steering away from uh the IC community because uh I haven't been involved in in quite a while there's really no point it's actually misleading. For those who see that language. Um, I don't want to waste anybody's time. And uh really, um but it's it's a constant care and feeding of my public profile to present the most accurate up to date and uh harmless um public presentation that I can um you uh to uh you know benefit those in my network and uh and myself to be honest." (11205114603, ERRS02, 3)
	GPCN	A	"I don't friend everybody asked to be friended I think you asked and I did for you. But uh just because of the topic you were working on, buty yeah, I mean, I don't if I don't know the person" (11269613365, GPCN03, 3)
		H	Not Represented
	INVN	A	Not Represented
		H	"I've actually as an aside, I've had my identity stolen on Facebook, in one of these romance scam things and I had four to 500 uh fake profiles out there and people contacting me etc, which gave me great stress." (11224014306, INVN05, 2)

(continued)

Topic	Code	OG	Snippet
Topic Four, "Finally, let's discuss your intention to modify your LinkedIn profile's visibility." (continued)	PRBF	A	"I also realize that people that know know people that I know can see my some of my stuff because they, they share it. So, once again, I uh it's my assumption that anything that's on those sites is going to be open source to anybody. " (11269613365, PRBF11, 2) "No, once again, I just it's my opinion that if I put something on a link on a link like LinkedIn so I would say something like clearancejobs.com all of them. Yeah, I mean it would I follow the rules the government has given me and that and then I would expect it to be open source anybody that looks at those sites that once again, I don't let every I don't." (11269613365, PRBF13, 2.5) "Even when you send an email, you know, to a friend, you're not necessarily secure all the time, but that's a whole different problem where people have hacked into people's email accounts." (11269613365, PRBF23, 3)
		H	Not Represented
	USGE	A	"I don't know what they're doing with the data, then I'm pretty I close it down pretty, pretty uh tightlly." (11269613365, USGE03, 3)
			"And I believe that uh people generally generally are doing the right thing and abiding by the terms of service and uh and why they're using the system. But I know that that is not always the case." (11223476508, USGE06, 3)
		H	Not Represented
Topic Five, "Are there any other additional thoughts or comments you might have?"	BNFT	A	"So I'm not there's not a lot of hiding unless I go, you know, off grid and I'm not willing to do that, the benefit is worth the uh um uh the effort." (11188138618, BNFT07, 3)
		H	Not Represented
	COLL	A	"Uh um there is a way that they could probably figure out my birthday. But you know, again, there's so much public knowledge out there that for a few dollars at a time, you could put together a fairly decent um uh biography of [NAME REMOVED]." (11188138618, COLL01, 3)
		H	"I think as we're moving forward and gaining more capabilities in our and an the ways that we're able to collect and store data." (11224014306, COLL06, 3)
	CNTL	A	"They uh you know, do I give them my social security number? No, do I give them my uh um birthday?" (11188138618, CNTL03, 3) "So people have to take a personal uh position on what they're doing, what they're posting out there." (11269613365, CNTL04, 2) "So you gotta, you kind of gotta filter what you're saying and doing and uh uh its kinda, I don't think ther's any expectation." (11269613365, CNTL05, 2.5) "I don't give out explicit personal information but um you know, people know my phone number because uh they know my phone number or they know my address because it's public record." (11188138618, CNTL08, 3)
		H	Not Represented

(continued)

Topic	Code	OG	Snippet
Topic Five, "Are there any other additional thoughts or comments you might have?" (continued)	ERRS	A	Not Represented
		H	"So this is for me this is a good reminder to go back in there and double check on things to make sure that uh the image that I'm trying to present is a s professional and uh accurate as possible." (11205114603, ERRS04, S)
	INVN	A	Not Represented
		H	"And I want to cut back on some of this other stuff. Uh, especially as I get older, I don't want to be losing a nickel to anybody who uh may steal my stuff. I lost 25 thousand dollars a few years ago, though, was FDIC a little bit of a ramble there." (11224014306, INVN04, 3)
	PRBF	A	"I'm uh basically I'm hiding in the, in the in the vast, you know, expanse I mean than vice trying to make it active uh [undecipherable distortion]." (11188138618, PRBF01, 2.5) "So it's a social media site. So anyway, and I know there's a lot, a lot of millennials, I guess there's an expectation of these things to be more than what they were intended to be, I think, so. These expectations evolve. And I don't really know what the foundation for it is why they believe that." (11269613365, PRBF09, 3) "Um nuh nothing but to, you know to say in my viewpoint and I think this is pretty clear from the interview, I I deem any anytime that I enter into the internet, whether it's through LinkedIn or Facebook or uh an email, or whatever, um I do not consider unless I go to extreme means to encrypt and uh hide emails uh through VPN or encryption software. And I don't I don't consider uh um myself to be as secure. So whatever I'm saying or doing, uh um I I fully intend to be looked at." (11188138618, PRBF12, 3) "I don't have any expectation of privacy on any of those sites." (11269613365, PRBF24, S)
		H	Not Represented

(continued)

Topic	Code	OG	Snippet
Topic Five, "Are there any other additional thoughts or comments you might have?" (continued)	REGL	A	Not Represented
		H	"And and um I guess it's frustrating from a jurisprudence perspective on the exactly what mechanisms are in place to um prosecute, uh certainly into the, you know, the digital cyber realm, um which, which is tough to, and then the content could potentially be classified, which adds another uh layer to another dimension to prosecution. Uh and again, I think uh, using Julian Assange um and the Wikileaks program as as a whole, using that model, uh and then seeing that uh its taken 10 years to to bring him to trial, uh I think speaks poorly of, of our um our government's ability to uh provide ramifications for such activities." (11251351842, REGL02, 2.5) "But, um, I think we need to relook things and starting with many of the laws that are in place and the ability to collect on on Americans, and then also the ability for private companies to collect on us also." (11224014306, REGL04, 3) "I know we sign an I agree thing, but nobody reads any of that stuff. Uh, I think that is us that's very concerning to me." (11224014306, REGL06, 3) "Uh, American and American lawmakers need to take a look at uh what we're allowing companies to do and selling data." (11224014306, REGL09, S)
	USGE	A	Not Represented
		H	"I do think there needs to be a very hard look at what they can do with our stuff without permission." (11224014306, USGE04, 2.5) "The probably in in in stepping back it uh this is not the first time that uh an entity agency has looked to scrape and or um use this information for, you know, malicious type attacks." (11251351842, USGE14, 3) "Uh, you know, we just another point, I have friends who do this DNA testing, which I will never do because I don't know who's going to get ahold or protect my DNA somewhere. Might be some guy in China walking around with my DNA, so I don't do that." (11224014306, USGE15, 2.5) "Uh, and I know they do that at Facebook for promotional concerns and stuff like that." (11224014306, USGE17, S)

Note. Snippet details provided after each in the following format: Participant ID, Code ID, Validation Score. S= validation sample snippet

Appendix E

Interview Transcripts

The following are transcripts of the six Phase 2 interviews. Each interview was recorded via Zoom. The audio files were uploaded to a transcription service call Otter.ai. Using the real-time editing tools, transcripts were reviewed through multiple rounds to ensure accuracy. A subsequent validation review was conducted by an independent auditor to ensure transcription accuracy. A separate validation review was conducted to ensure that individual snippets were uniquely associated with only a single code, and highlighted.

Interview 11188138618

Sat, 4/18 8:33AM

SPEAKERS
John Marsh, 11188138618

John Marsh 15:17
Hello.

11188138618 15:17
Hello, Hey, how you doing Mr. Marsh?

John Marsh 15:23
Very well, thank you. Are you participant 11188138618?

11188138618 15:32
Yes.

John Marsh 15:34
Perfect, and do you consent to be interviewed?

11188138618 15:38
Yes, I do.

John Marsh 15:40
And do you consent to this interview being recorded?

11188138618 15:43
Yes.

John Marsh 15:45
Perfect, so please allow me to explain this study for a few minutes briefly. Its purpose is to investigate the linkages between privacy and behavior in an actual privacy specific scenario. If you will recall you previously took a survey regarding your LinkedIn profile data being scraped and posted to a third party's website called ICWATCH. Per their website, ICWATCH is a project to collect and analyze resumes of people working in the intelligence community. People working for intelligence contractors, the military and intelligence agencies frequently mention secret code words and surveillance programs in public resumes. These resumes are useful for uncovering new surveillance programs, learning more about known code words, identifying which companies help with which surveillance programs, examining trends in the intelligence community and more. This study is designed to examine the level of an individual's disposition to value privacy, how this influences their situational privacy concerns regarding their information being scraped, and posted by ICWATCH, and ultimately, its influence on the users intentions modify their LinkedIn account settings. So now I will capture your feedback on several topics for a few minutes each. You are welcome to ask me to rephrase or explain anything. Are you ready to proceed?

11188138618 17:06
Yes, sir.

John Marsh 17:08
Perfect. Uh, so topic one, for the next few minutes let's discuss if this situation is a breach of privacy. What are your thoughts?

11188138618 17:20
The situation that we're in now?

John Marsh 17:22
Uh the your information being scraped from LinkedIn and being posted on ICWATCH.

11188138618 17:29
•[PRBF07]No, cuz uh and and the reason why I believe that is when you join LinkedIn, you give up inherent uh um rights to privacy by stepping into LinkedIn.

John Marsh 17:44

All right, give me one moment. All right, uh topic two. For the next few minutes, let's discuss your disposition to value privacy. What are your thoughts?

11188138618 18:02
•[CNTL16]Um, if I want privacy, then I don't engage that's the only way to secure absolute privacy. •[PRBF20]Um so uh I don't um believe that knowing my name, and uh, and uh knowing my disposition, but through conversation, either over the phone or uh, or in person is anything more than just um that person that I'm engaging with, using their uh, their skills and their uh techniques of a, of a um observation to to make a make a deduction. •[CNTL02]So if if I don't want uh, if if I want to be private, that I don't engage, that's, that's the only way to be completely private. •[PRBF25]And uh so um when I say that, you know, I'm gonna engage somebody um through a conversation, I'm willing, uh at that point I made a decision that I'm gonna give up some of my property to go uh um further. So um I'm, I I engage clients all day long with uh conversations regarding, uh you know, products and services, uh and [undecipherable distortion] then sometimes make connections and I'm always looking at them to uh get [undecipherable distortion] um uh fissures into their, um uh I guess, into their uh, their their [undecipherable distortion], to make a um determination on uh you know, most effective to get uh my across and to get them to uh um uh be sympathetic, if not absolutely um uh convinced that I have the best product for them.

John Marsh 20:17
Alright, perfect. Uh, for the next few minutes, let's discuss your level of concern regarding ICWATCH scraping and posting your data.

11188138618 20:26
•[PRBF19]Uh, again, you know I uh my concern is a, is really kind of moot um as I engage in those already um when uh when I decided to go onto LinkedIn, you know, I I knew um that uh there was going to be a um uh the disability because I I knew of this ability to scrape information and and uh um you to fit into algorithms that would be able to uh ascertain my likes, dislikes, and and basically pull the strings, my personality. •[PRBF14]So, you know, again uh, you know, I made the conscious effort, uh the conscious decision that that what they were going to be able to ascertain from me was uh not going to directly uh um affect me and uh in a negative way and and not to negatively uh affect me in an indirect ways either. Um I don't think that a uh bad actor could um necessarily get enough information to do do me or my um family harm. Um, but you know, I'm I am semi prepared uh if if that case ever comes to fruition.

John Marsh 22:04
Alright, give me ne moment. Just taking some notes.

11188138618 22:13
Sure.

John Marsh 22:15

Alright then topic four. Finally, let's discuss your intention to modify your LinkedIn profiles visibility.

11188138618 22:25
•[BEHV08]I don't I don't have plans right now. •[BNFT01]Uh, I uh I, I may be looking for another job soon. So, I am uh going to um hazard to keep the the line of communication open, uh no changes, uh updating some of my uh um CV there and uh just you know um reaching out to people that I deem worthy uh in my um search for a a better job and or uh um to further further me in the job already have. •[BEHV04]So, you know, I'm not I'm not um anticipating any changes.

John Marsh 23:12
Alright. And uh do you have any final thoughts or additional comments on anything we discussed?

11188138618 23:21
•[PRBF12]Um nuh nothing but to, you know to say in my viewpoint and I think this is pretty clear from the interview, I I deem any anytime that I enter into the internet, whether it's through LinkedIn or Facebook or uh an email, or whatever, um I do not consider unless I go to extreme means to encrypt and uh hide emails uh through VPN or encryption software. And I don't I don't consider uh um myself to be as secure. So whatever I'm saying or doing, uh um I I fully intend to be looked at and •[PRBF01]I'm uh basically I'm hiding in the, in the in the vast, you know, expanse I mean than vice trying to make it active uh [undecipherable distortion]. •[CNTL08]And I don't give. I don't give out explicit personal information but um you know, people know my phone number because uh they know my phone number or they know my address because it's public record. •[CNTL03]They uh you know, do I give them my social security number? No, do I give them my uh um birthday? •[COLL01]Uh um there is a way that they could probably figure out my birthday. But you know, again, there's so much public knowledge out there that for a few dollars at a time, you could put together a fairly decent um uh biography of [NAME REMOVED]. •[BNFT07]So I'm not there's not a lot of hiding unless I go, you know, off grid and I'm not willing to do that, the benefit is worth the uh um uh the effort.

John Marsh 25:23
All right. Uh well, thank you again for your participation. This concludes my data collection.

11188138618 25:29
I appreciate

Interview 11205114603

Sat, 3/28 2:49PM

SPEAKERS
John Marsh, 11205114603

John Marsh 07:21
Hello,

11205114603 07:23
Hello, can you hear me?

John Marsh 07:26
I can. Can you hear me?

11205114603 07:27
I sure can took me a minute to figure out this contraption but I got it.

John Marsh 07:32
Oh no worries whatsoever. So I just want to confirm that you are participant 11205114603

11205114603 07:43
That is correct.

John Marsh 07:46
And do you consent to be interviewed?

11205114603 07:51
Yes, yes I do.

John Marsh 07:53
Okay, and do you consent to this interview being recorded?

11205114603 07:57
Yes.

John Marsh 07:59
Perfect. Uh, so please allow me to explain this study for a few minutes briefly. Its purpose is to investigate the linkages between privacy and behavior in an actual privacy specific scenario. If you will recall, you previously took a survey regarding your LinkedIn profile data being scraped and posted to a third party website called ICWATCH. Per their website ICWATCH is a project to collect and analyze resumes of people working in the intelligence community, people working for the intelligence contractors, the military and intelligence agencies frequently mention secret code words

and surveillance programs in public resumes. These resumes are useful for uncovering new surveillance programs, learning more about known code words identifying which companies help with which surveillance programs examining trends in the intelligence community and more. This study is designed to examine the level of an individual's disposition to value privacy. How this is influences their situational privacy concerns regarding their information being scraped, and posted by ICWATCH, and ultimately, its influence on the user's intention to modify their LinkedIn account settings. So now I will capture your feedback on several topics for a few minutes each. You are welcome to ask me to rephrase or explain any of the questions or topics. Are you ready to proceed?

11205114603 09:26
Yes.

John Marsh 09:28
All right, perfect. So for the next few minutes, let's discuss if this situation is a breach of privacy. What, what are your thoughts on that?

11205114603 09:42
Oh, this situation you described?

John Marsh 09:45
Correct.

11205114603 09:46
Um, yes and no. Um, and I'll explain that real quick. •[BNFT10]Uh, on the one hand, people people put all sorts of stuff on their profiles um, in the effort to either get seen, get approached for work, establish a professional network or any number of things. •[COLL15]On the other hand, uh, I'm not sure many people realize that whatever they put out there is being um scooped up by whatever um artificial uh aggregators for lack of a better word, um to assist uh whatever agency creates those aggregators. •[PRBF06]Uh, so while while it's not a privacy issue, because you're volunteering to put your stuff out there, it's an argument could be made, it's in the public domain. •[COLL14]On the other hand, if you're not aware that your stuff is getting scooped up like that, maybe it's an issue for some Um, frankly, •[BEHV06]I'm torn on the subject. Um, after, after we, after we um engaged in our first um email conversation and exchange of information, I went back and looked at my stuff. And I think I made some adjustments and I'm still it's a constant, constant thing as, as uh life professional and personal changes, you you make adjustments to those public profiles you make, to adjust to those changes um for good or bad or however •[SPCN02]Um, so, for me it's it's a double edged sword it could be construed as a privacy issue. While on the other hand, it might not be depending on on um the the exact nature of one your understand you as an individual your understanding of what those profiles are and are used for and two, the information you're putting out there.

John Marsh 12:05
Okay, um so for the next few minutes, let's discuss your disposition to value privacy.

11205114603 12:16
Okay. Is it a question?

John Marsh 12:21
What are your, this is mostly topics. So really what I want to know is, you know, how do you value privacy and uh what is your approach to or your feelings about privacy online, personally?

11205114603 12:39
•[GPCN01]Um, I do value privacy. •[CNTL14]And for that reason I don't have the only social media outlet I have is LinkedIn. •[BNFT03]And I established that for a specific reason. Which has evolved over time. •[CNTL01]Um, I don't, I don't care to put much information out about myself. That's just my nature. •[SPCN05]I never have been that way, whether before the internet or even even today, so it's not really uh, for me, it's not really a privacy specific issue. It's more of a personality and I guess the nature of me issue. •[PNTR02]I'm not a very uh outgoing or extroverted person, •[GPCN07]I don't feel the need to share my life with strangers. •[PRBF05]Um, with that said, I do realize that uh let's let's put it this way, the, my philosophy is um, if you don't want people to know something, don't put it on the internet. •[PRBF16]Because once it's out there, you lose complete control over it. It's no longer yours. you're you're you're on someone else's platform, therefore, it's at least partially theirs and they can do with it. What they want. If you're okay with that, then the rules governing privacy are a little bit looser. Uh, if you're not okay with that, don't use a platform. •[PRBF22]Uh, but, but for me, as soon as you put information out there, you, you lose control of it. So just a matter of risk you're willing to accept, accept that risk. Go for it. I or, •[PNTR01]for me, I just don't find that myself that interesting to put so much information out there uh for •[ERRS01]professional reasons I had to and uh but every now and then I go back in there and I make some adjustments, make some updates, take some stuff off that are no longer relevant. Um, but that's, that's my uh, that's my take on on it, especially with regard to the internet and LinkedIn.

John Marsh 14:54
All right, perfect. Um, so for the next few minutes, let's discuss your level of concern regarding ICWATCH scraping and posting your data.

11205114603 15:04
•[SPCN04]Okay, yeah, that was a surprise to me. Um, I, at first I was I was uh, I was quite unhappy about that. But on the other end, I went back to my original philosophy. Well, I put the stuff out there. Um, and I immediately went back in there and looked to see what terms and words I used to attract potential recruiters. •[BEHV02]And I think I went back there and uh did a general scrub and use more general terminology, because I'm not I'm no longer in that in that profession. So there's, there's really no need to attract that attention. •[SPCN01]Um, on the other hand, it was it was the more I thought about it, the more I realized, well, that's to be expected. •[USGE10]Uh, for whatever purposes um, you know, could be nefarious, it could simply be trying to find the right people for the right position across the IC uh or other other agencies, private and public. •[ERRS03]But uh, but

for me, I have no need to be in that um in that world anymore. Uh, so as time goes on I, I remove a lot of those specific key terminologies simply because um that's in the past and it's no longer relevant.

John Marsh 16:34
Perfect. Uh, and then finally, let's discuss your intention to modify your LinkedIn profiles visibility.

11205114603 16:42
•[BEHV09]Okay, yeah um. I plan on I don't do it as frequently as I should. But uh not, uh not because of you specifically, or the subject matter. But yeah, before the weekend. I'll probably go back in there and um take another look and see what, what not image but •[BNFT04]what public profile of me I want out there to strengthen or expand my network. Take it in the direction I want it to go. •[ERRS02]Um, as I mentioned before, I'm definitely uh steering away from uh the IC community because uh I haven't been involved in in quite a while there's really no point it's actually misleading. For those who see that language. Um, I don't want to waste anybody's time. And uh really, um but it's it's a constant care and feeding of my public profile to present the most accurate up to date and uh harmless um public presentation that I can um you uh to uh you know benefit those in my network and uh and myself to be honest. So yes, before probably before the weekend is out, I will have gone back in there and taken another look.

John Marsh 18:19
All right. Um, so is there any uh other thoughts or additional comments you'd like to add based on uh some of the topics you've discussed?

11205114603 18:28
Um, I think if anything is pretty cut and dry to me, I think I've explained my position and the thinking behind it. And the uh in my approach going forward. Um, It's good to have these reminders that there are constantly organizations and people out there looking looking at the at the things you put online. Um, It's a constant uh reminder that care should be taken not only for um the profession, but also, uh you know, in your personal life. Um, you don't want to um you don't want to drag your baggage out in the real world because it will it will come back to haunt you um especially as you're seeking um professional uh expertise and, and uh work and things like that. •[ERRS04]So this is for me this is a good reminder to go back in there and double check on things to make sure that uh the image that I'm trying to present is as professional and uh accurate as possible.

John Marsh 19:53
Perfect. uh so uh, thank you again for your participation. Uh this concludes my data collection.

11205114603 20:01
All right, thank you very much

Interview 11223476508

Sat, 3/28 2:56PM

SPEAKERS
John Marsh, 11223476508

John Marsh 11:04
Hello.

11223476508 11:06
Hi there. How are you?

John Marsh 11:08
Oh, very well. Uh, good evening are you participant 11223476508?

11223476508 11:17
I, I'm assuming so that was in the email.

John Marsh 11:21
Okay. Fair enough. And do you consent to be interviewed?

11223476508 11:26
Yes, I do.

John Marsh 11:28
And do you consent to this interview being recorded?

11223476508 11:31
Uh, yes, I do.

John Marsh 11:34
Perfect. Uh, so please allow me to explain this study for a few minutes briefly. Um its purpose is to investigate the linkages between privacy and behavior in an actual privacy specific scenario. If you will recall, you previously took a survey regarding your LinkedIn profile data being scraped and posted to a third party website called ICWATCH. Per their website, ICWATCH as a project to collect and analyze resumes of people working in the intelligence community. People working for intelligence contractors, the military and intelligence agencies frequently mention secret code words and surveillance programs in public resumes. These resumes are useful for uncovering new surveillance programs, learning more about known code words, identifying which companies help with which surveillance programs, examining trends in the intelligence community and more. This study is designed to examine the level of an individual's disposition to value privacy, how this influences their situational privacy concerns regarding their information being scraped, and posted by ICWATCH. And ultimately, its influence on the user's intention to modify their LinkedIn account settings. So now I'll

capture your feedback on several topics for a few minutes each. You're welcome to ask me to rephrase or explain anything? Are you ready to proceed?

11223476508 13:05
I am. Yes.

John Marsh 13:07
Perfect. So for topic one, uh for the next few minutes, uh let's discuss if the situation is a breach of privacy, what are your thoughts?

11223476508 13:18
•[GPCN04]So I post information on the internet with no expectation of privacy. •[PRBF21]I fully am aware that the information that I post to any public page is available to any person. •[CNTL17]Uh, I my resume is an assemblage of my life experience and I have not divulged any classified information. In fact, that resume was scrubbed and approved for release prior to it being posted anywhere or used for my job search. •[PRBF08]And so I was fully aware that both LinkedIn would use my information, as well as the availability of that information to others uh uh or whoever scraped or used or viewed that information, •[PRBF04]there was never an expectation on my part that that information would be considered private or protected in any way.

John Marsh 14:33
All right. Um, so for topic number two, for the next few minutes, let's discuss your disposition to value privacy.

11223476508 14:45
•[GPCN06]So, I, uh I value my privacy, and •[CNTL15]I take steps to ensure that what I post or provide to others is information that I intend to provide that, that I've thought about the implications of that information and the, the uh, you know, the receiver of that information and and uh those sorts of contingencies or outcomes, and so um and •[GPCN05]so that so I consider myself a very private person in that regard in that. •[CNTL18]I, I do not post a lot of social media information. •[CNTL19]I have a Twitter account, but I don't tweet you know, I mean, I um so, I don't, I don't provide a lot of information, because I consider much of that private.

John Marsh 15:57
Perfect. Uh, for topic number three For the next few minutes, let's discuss your level of concern regarding ICWATCH scraping, posting your data.

11223476508 16:10
So, so in regard to the topic that we're discussing, I have no concern at all about my information being posted. •[USGE09]Uh I believe that IC I don't know where ICWATCH is located or the people that are involved in it, but they potentially make it easy for enemies of the United States to assemble information. Now, that information is obviously, you know, available out there. •[COLL12]But it does uh provide a central repository for somebody who's interested and desires to have introspection into the US intelligence

community. Um, your thesis statement talks about, um you know, code words and different information and the assembly of aggregate information and, and I, I believe that that is an issue in uh general that the, you know, a lot can be learned from uh, from assembling different data sources and analyzing those. And um so, at some point, you know, we are as a, as a human race going to really have to come to grips with the understanding of what privacy is because because of the potential for these different data sets to be assembled and for people to resolve and to make different judgments and understand different aspects of life, how people live, what they do, how they think um, and it happens now in the ad tech world. •[COLL07]Uh, you know, the things that Facebook and I, I mean, it's just it's out there already and people have a a limited understanding of the totality of the knowledge that's uh available to a company like Facebook or to LinkedIn or to to others who have assembled these datasets and uh conducted analysis on them.

John Marsh 18:34
All right. And then uh finally, let's discuss your intention to modify your LinkedIn profiles visibility.

11223476508 18:41
•[BEHV11]Uh, I do not intend to change anything. I update my resume periodically. I don't intend to change any settings. •[BNFT05]I accept nearly all requests to uh know whenever it's not a friend request that leaked at LinkedIn but but I I think there's value in networking. •[USGE06]And I believe that uh people generally generally are doing the right thing and abiding by the terms of service and uh and why they're using the system. But I know that that is not always the case. •[BEHV01]But uh I'm not intending to change anything. And like I said, I accept almost all requests for access and network.

John Marsh 19:44
Alright, I'm just taking some notes real quick.

11223476508 19:46
Certainly.

John Marsh 19:50
Um, so with that uh, any, any uh additional comments or thoughts based on the topics you discussed?

11223476508 20:01
No I think we've pretty much covered everything.

John Marsh 20:05
All right. Um, so thank you again for your participation. This concludes my data collection.

Interview 11224014306

Thu, 3/12 8:34PM

SPEAKERS
John Marsh, 11224014306

11224014306 00:00
Sure am great.

John Marsh 00:03
All right, perfect. Well uh, let me start by saying Good evening, and um I'll capture your participant ID but I'm assuming since you're in your car, you probably don't have it handy.

11224014306 00:14
Uh no, I don't, well, let me see

John Marsh 00:19
It's not terribly important. I was just trying not to capture names if I didn't have to, but I cannot.

11224014306 00:25
Okay. It's uh, I have it. It's 11224014306.

John Marsh 00:37
Perfect. Thank you. And do you consent to be interviewed?

11224014306 00:42
Yes, and I sent you the forms last night.

John Marsh 00:46
And I did receive them. And I just wanted to also capture do you consent to this interview being recorded?

11224014306 00:53
Yes, Yes, I do.

John Marsh 00:55
Alright, perfect. Uh, so just allow me to briefly explain uh this study real quick.

11224014306 01:01
Okay.

John Marsh 01:02

So its purpose is to investigate linkages between privacy and behavior in an actual privacy specific scenario. If you will recall, you took a survey regarding your LinkedIn profile data being scraped and posted to a third-party website called ICWATCH.

11224014306 01:19
Yes

John Marsh 01:20
Per, per their website ICWATCH is a project to collect and analyze resumes of people working in the intelligence community. People working for intelligence contractors and military and

11224014306 01:35
Okay,

John Marsh 01:35
These resumes, these resumes, go ahead

11224014306 01:40
I used to, I don't work for the IC anymore. Is that okay?

John Marsh 01:44
Oh, oh, absolutely. That's fine um these resumes, per ICWATCH the resumes are useful for identifying people in the intelligence community.

11224014306 01:57
Okay,

John Marsh 01:58
So, specifically, my study is designed to examine the level of an individual's disposition to value privacy.

11224014306 02:06
Okay

John Marsh 02:07
How this influences their situational privacy concerns related to having their information scraped and posted by ICWATCH, and ultimately, its influence on the user's behavioral intention to modify their LinkedIn account settings.

11224014306 02:22
Okay.

John Marsh 02:24

All right. Um so um I will capture your feedback on the following topics for a few minutes each. And you're welcome to ask me to rephrase or explain anything. Are you ready to go?

11224014306 02:37
Uh ready to go.

John Marsh 02:40
Perfect. Um so for the next few minutes, uh let's discuss if you, if this situation is a breach of privacy,

11224014306 02:49
Okay

John Marsh 02:51
What do you think? Did you believe this is a breach of your privacy?

11224014306 02:55
What the scraping of the uh, of my site, of LinkedIn?

John Marsh 03:02
Correct the scraping of your site and then having that information posted to ICWATCH.

11224014306 03:09
•[INVN01]Yes um yes and no, I'm sorry, I've have to answer it that way. •[BNFT06]I, I am on LinkedIn, which is an open site and I people use that to find resumes and things like that. Um, so in that respect, I'm fine uh, because I'm looking for something that's advantageous to me. •[USGE13]But I don't know what's going on on this site where my information is going. •[SPCN07]So I do feel that uh, a little concerned about that based on what I know about Intel communities and sharing of information.

John Marsh 03:47
Okay, great. Uh, so for the next few minutes uh let's discuss your disposition to value privacy.

11224014306 03:57
Okay, um I value my privacy, uh especially in this day and age. Um, let me just go back a few years after 911 when I was a younger guy, and even before that, I really didn't have a lot of concerns about privacy necessarily. Ah because things weren't in place, uh I what's the word I'm looking for intelligence, ability to grab information, uh the the social networks and all those sorts of things were not in place. So I really felt very comfortable uh in in giving information out in presenting it. Ah, those were the days when you could actually keep your social security number on ah on your check and pass it around freely. Ah, then 911 hit and ah I was ah I was in agreement that we should have much more of a robust intelligence ability to go after terrorists and those people who are ah possibly criminals in the United States and those who are outside. •[COLL03]But as time has gone by,

and much more sophistication, on the ability to grab data from us all kinds of information, and •[INVN06]I've been hacked and lost a lot of money about five or six years ago, and I thought I think it was from the Chinese, ah based on some, some uh research I did, •[SPCN08]I become quite concerned, also concerned with little funny things that happen when ah I'm standing around talking about a subject and it shows up on my ah Amazon feed or something of that nature. •[USGE12]So ah somebody's grabbing my information, ah somebody's using it for whether it's sales, or whether to rob me or use my uh uh social security number. •[INVN07]I was ah hacked through the OPM hack a couple of years ago, and God knows who has my Social Security numbers and things like that. •[GPCN02]So, ah right now, at this point, I'm very concerned about my privacy and •[REGL05]actually was a little disappointed when the Patriot Act was ah, I think if I'm not mistaken, I know it's being re-looked, I think it may have been approved, but I'm not sure we've made any adjustments on that. For our, our, our new um for this period, any updates, if you will, excuse me. Um, •[SPCN09]so yes, I'm concerned, did that make any sense?

John Marsh 06:34
It made perfect sense.

11224014306 06:36
Okay.

John Marsh 06:39
Alright. So moving on to the next topic. Let's discuss your level of concern regarding ICWATCH, scraping and posting your data.

11224014306 06:50
•[USGE05]Well uh, what are they doing with it? •[SPCN03]Uh, it does bother me. Um, when I first saw it, I was concerned. •[COLL11]Uh, it does bother me because I don't know what they're doing with I know what the NSA programs are with phones and things like that of gathering data uh and and uh holding on to it, but only looking specifically when they need something. Um, I don't feel comfortable with somebody holding on uh to critical information about me, what are they using it for? What are they scraping it for? And what are they doing with it? •[COLL05]So uh I think I need some questions answered, um before I can move forward in having worked in the IC community for a short period of time, just a couple years, I know the capabilities of what they can do and and uh things they can look at. •[SPCN06]And it makes me concerned. I just don't, uh I just don't have enough information about it. •[USGE08]So I guess my question, you know, if I'd summed up in one statement, what are you doing with it?

John Marsh 08:00
Sure, Okay, then moving on to the final topic, uh let's discuss your intention to modify, your LinkedIn profile's visibility.

11224014306 08:11
•[BEHV05]Yeah, that's funny you bring that up. Uh, aside from this, I was, someone had mentioned something like this just the other day I forget the specific, but um I, I, I

thought I was in a private mode, I'm going to have to take another look, not just with my LinkedIn, but also with Facebook and a few other things. •[INVN05]I've actually as an aside, I've had my identity stolen on Facebook, in one of these romance scam things and I had four to 500 uh fake profiles out there and people contacting me etc, which gave me great stress. •[BEHV03]So I i toned that thing down. And I uh think I uh may be doing the same with uh LinkedIn. •[BNFT11]I don't have a lot of information on there except of who I am, uh jobs i've held, which is advantageous to me. Uh, well was previously I'm 61 years old. •[BEHV10]I'm not going to be job hunting a lot more late in the next few years, but I, I think I'm going to take another look at it and see what is accessible. •[COLL08]Um again, I don't know, they're we're looking at if they've taken everything, um IP addresses, any phone numbers that may or may not be in there. Anything, anything I may have said. Uh, gives me pause. Okay.

John Marsh 09:34
Sure, give me one second.

11224014306 09:42
All right.

John Marsh 09:46
All right um. So is there any other additional thoughts or comments you might have?

11224014306 09:54
•[COLL06]I think as we're moving forward and gaining more capabilities in our and and the ways that we're able to collect and store data. •[REGL09]Uh, American and American lawmakers need to take a look at uh what we're allowing companies to do and selling data. •[USGE17]Uh, and I know they do that at Facebook for promotional concerns and stuff like that. •[USGE04]I do think there needs to be a very hard look at what they can do with our stuff without permission. •[REGL06]I know we sign an I agree thing, but nobody reads any of that stuff. Uh, I think that is uh that's very concerning to me. •[USGE15]Uh, you know, we just another point, I have friends who do this DNA testing, which I will never do because I don't know who's going to get ahold or protect my DNA somewhere. Might be some guy in China walking around with my DNA, so I don't do that. •[INVN04]And I want to cut back on some of this other stuff. Uh, especially as I get older, I don't want to be losing a nickel to anybody who uh may steal my stuff. I lost 25 thousand dollars a few years ago, though, was FDIC a little bit of a ramble there. •[REGL04]But, um, I think we need to relook things and starting with many of the laws that are in place and the ability to collect on on Americans, and then also the ability for private companies to collect on us also.

John Marsh 11:21
All right, uh perfect. Um, so, I'd like to say thank you again for your participation. This concludes my data collection.

11224014306 11:32
Okay,

Interview 11251351842

Sun, 4/5 8:04AM

SPEAKERS
John Marsh, 11251351842

John Marsh 06:47
Hello

11251351842 06:50
Hey how are you?

John Marsh 06:52
Very well thank you. Are you participant? Oh, okay [participant enables video], I suppose we could do that. That's, actually I don't have a camera on this computer.

11251351842 07:04
[Lauging] All right.

John Marsh 07:07
But uh, are you uh participant 11251351842?

11251351842 07:16
I am.

John Marsh 07:18
Perfect. And do you consent to be interviewed?

11251351842 07:18
I do. I do.

John Marsh 07:22
And do you consent to this interview being recorded? Perfect. Uh so please allow me to explain the study for a few brief minutes. Its purpose is to investigate the linkages between privacy and behavior in an actual privacy specific scenario. If you will recall, you previously took a survey regarding your LinkedIn profile data being scraped and posted to a third party website called ICWATCH. Per their website, ICWATCH is a project to collect and analyze resumes of people working in the intelligence community, people working for the intelligence contractors, the military, and intelligence agencies frequently mentioned secret code words and surveillance programs in public resumes. These resumes are useful for uncovering new surveillance programs learning more about known code words, identifying which companies help with which surveillance programs, examining trends in the intelligence community and more. This study is designed to examine the level of an individual's disposition to value privacy, how this influences their situational privacy concerns regarding their information being scraped, and posted by

ICWATCH, and ultimately, its influence on the user's intention to modify their LinkedIn account settings. Now, I will capture your feedback on several topics for a few minutes each. You're welcome to ask me to rephrase or explain anything. Are you ready to proceed?

11251351842 08:42
I'm ready to go.

John Marsh 08:50
Perfect. So topic one., for the next few minutes let's discuss if this situation is a breach, breach of privacy. What are your thoughts?

11251351842 08:59
•[INVN02]So, the um the breaches the breach of privacy is actually an intrusion into the personal life of another specifically without just cause. •[REGL03]So I've submitted this particular instance, they do not have have just cause and and rather um the privacy that's being invaded, I would have, if you will, the essence uh or legal liability or legal uh ability to bring a lawsuit if damages or for damages that were incurred. •[GPCN08]Um, obviously, I'm not any celebrity or public figure who could reasonably assume to be recognized in the public and not be protected. But I would go on to say um that As a nonpublic individual, I uh certainly have the right to be protected from any intrusion on my solitude and my private affairs. •[USGE07]Uh, and then anybody that takes those, that data and disclose them in it with the intent to embarrass me or somehow discredit me with that private information causes us concern. •[USGE02]Um, so, the uh uh or uh in addition, takes that information and uh puts it in in the public under a false light. Uh, and then lastly, uh uses my name and or uh my personal information for some sort of uh uh commercial advantage. •[INVN03]So, so the breach of privacy is not fully satisfied, if you will, under under this particular uh situation. Under this particular topic, ie a breach of privacy, that they scraped my personally available information um that anybody with a reasonable uh basis could do you know, from uh Facebook, um and that is made to the general public, certainly. Uh, but does that necessarily constitute a breach of my privacy? Uh, no, not at this point.

John Marsh 09:50
Okay. Uh, take some notes for a minute.

11251351842 11:32
Okay.

John Marsh 11:34
Okay. All right. So moving on to topic two, for the next few minutes, let's discuss your disposition to value privacy.

11251351842 11:44
Okay. •[GPCN09]Uh, at the end of the day, I certainly value the right to be left alone. •[PRBF17]Uh my personally identifiable information is uh um thought to be at least

protected from public scrutiny, especially as a employee of the government, uh but I think uh recent breaches with, especially with the Office of Personnel Management has almost made that null and void. •[REGL08]Um and certainly looking through the uh amendments, probably the closest one that covers any sort uh of privacy information uh is both the 14th amendment uh or more importantly the Privacy Act of 1974 uh which in theory should prevent the unauthorized disclosure uh held by the government. Um, so, so, uh so in some value it protections are in place. Uh, are they being followed is the spillage occurred? Certainly. Uh does that uh help or hurt uh ICWATCH. Um, you know, •[COLL09]I, I suspect the bigger the bigger issue and bigger concern um would be to take uh the information from the OPM or some of the other databases that have been breached and and kind of uh meld them together if you will.

John Marsh 13:21
Okay. I'm sorry. So moving on to topic three for the next few minutes, let's discuss your level of concern regarding ICWATCH scraping and posting your data.

11251351842 13:38
Okay. •[SPCN10]Um, surely, uh ICWATCH um their behavior certainly raises red flags. •[USGE16]Um and at the end of the day, the question comes into uh what the intent is, um you know, is the intent malicious Um, that's questionable. Uh is I would say that posts in any of my information is less than desire desirable, certainly. Um, to be sure, I know the information I had on my profile is sanitized to the fullest extent possible. •[USGE11]Um, using the WikiLeaks model as a conduit to the general public, um um it was in my mind anyways that that uh that breach that scraping of information that technique that model is uh designed more clear or clearly more designed, if you will, to harm the IC community and and writ large the US government. •[REGL07]Um, so um you know, the the fact that ICWATCH has violated personal privacy in the past it has and and and, more importantly, the US government's resolve to do anything about it. Um um you know, has has me equally concerned and I say that because uh uh Julian Assange uh has been uh under um has not been brought to trial in 10 years despite being uh currently at trial as we speak. •[USGE01]Um but uh you know, his his model of behavior, not only with ICWATCH, but similar programs were designed to do that bring discredit on um the folks in that community. So it does raise a red flag. They could certainly be used um with a nefarious attack. •[REGL01]Um um but but looking at the some of the previous models, um especially with uh Chelsea Manning, and and uh and others. Um it it certainly did harmful and uh severe damage to the US government writ large. Uh, but at the end of the day, uh I think uh the uh WikiLeaks enterprise and especially Julian Assange, have perhaps a more personal uh price to pay.

John Marsh 16:33
All right. Uh then finally, let's discuss your intention to modify your LinkedIn profiles visibility.

11251351842 16:42
•[BEHV07]Um, so quite honestly, I like it the way it is, •[BNFT02]I scrubbed it uh even before this couple of weeks, two three weeks ago uh with the intent of um ensuring um my

network of IC and uh intel professionals recognize um the new duties and positions that I was that I'm currently in. And then more importantly, uh should I opt to uh leverage those that skill set into other arenas other commands? Um I had the requisite background that was uh verifiable um for potential recruiters and what.

John Marsh 17:36
All right. Um, so any uh additional thoughts or comments you might have based on the topics that we discussed?

11251351842 17:51
•[USGE14]The probably in in in stepping back it uh this is not the first time that uh an entity agency has looked to scrape and or um use this information for, you know, malicious type attacks. •[REGL02]And and um I guess it's frustrating from a jurisprudence perspective on the exactly what mechanisms are in place to um prosecute, uh certainly into the, you know, the digital cyber realm, um which, which is tough to, and then the content could potentially be classified, which adds another uh layer to another dimension to prosecution. Uh and again, I think uh, using Julian Assange um and the Wikileaks program as as a whole, using that model, uh and then seeing that uh its taken 10 years to to bring him to trial, uh I think speaks poorly of, of our um our government's ability to uh provide ramifications for such activities.

John Marsh 19:21
All right. So um thank you again for your participation in the interview. This concludes my data collection.

Interview 11269613365

Sat, 3/28 2:54PM

SPEAKERS
John Marsh, 11269613365

John Marsh 07:23
Hello

11269613365 07:24
Hey John, [participant name removed].

John Marsh 07:27
Oh, hey, how you doing?

11269613365 07:28
Good.

John Marsh 07:30
All right. Let me start this out by saying good evening. Are you participant 11269613365?

11269613365 07:41
I am.

John Marsh 07:43
And do you consent to being interviewed?

11269613365 07:46
I do.

John Marsh 07:47
And do you consent to this interview being recorded?

11269613365 07:50
I do.

John Marsh 07:52
Perfect. So please allow me to explain the study for a few minutes briefly. Its purpose is to investigate

11269613365 08:00
Okay

John Marsh 08:01

Its purpose is to investigate the linkages between privacy and behavior in an actual privacy specific scenario. If you will recall, you previously took a survey regarding your LinkedIn profile data being scraped and posted to a third party website called ICWATCH. Per their website, ICWATCH is a project to collect and analyze resumes of people working in the intelligence community. People working for the intelligence contractors, the military and intelligence agencies frequently mention secret code words and surveillance programs in public resumes. These resumes are useful for uncovering new surveillance programs, learning more about known code words, identifying which companies help with which surveillance programs, examining trends in the intelligence community and more. This study is designed to examine the level of an individual's disposition to value privacy, how this influences their situational privacy. privacy concerns regarding their information being scraped and posted by ICWATCH, and ultimately, its influence on the user's intention to modify their LinkedIn account settings. So now, I will capture your feedback on several topics for a few minutes each, and you are welcome to ask me to rephrase or explain anything that isn't clear. Are you ready to proceed?

11269613365 09:24
I am.

John Marsh 09:26
Perfect. So the first topic for the next few minutes, let's discuss if this situation is a breach of privacy.

11269613365 09:36
Okay

John Marsh 09:37
What are your thoughts on that?

11269613365 09:39
I really don't think it is. So.

John Marsh 09:41
Okay.

11269613365 09:42
•[CNTL13]I think I told you that my questionnaire I think that, you know, you could have as much as an individual, I could have as much privacy as I want. •[PRBF03]But I think if you go out to social media sites, you gotta it's my position that you don't have any uh any expectation of privacy at that point. •[PRBF18]So, I mean, that's why they're called social media, right? So uh I guess that pretty much answers my the question. Yeah. Do you want me to elaborate any further on that?

John Marsh 10:18

Um, oh, no. If you have something you'd like to add, that's great. If not, uh however, you answer is perfectly fine.

11269613365 10:26
•[PRBF10]I just want to let you know, I can elaborate if you want more, but I just know that that's how I feel it just uh. You know, just by the term social media. So LinkedIn, Facebook, Twitter, all those are uh social media sites, and I have no expectation of privacy on any of those sites. •[PRBF02]Although they try to do it. I mean, it's just, I mean, I don't know how hard it would be to for their platform to work with uh personalized privacy settings. So I really don't expect, I have no expectation of privacy on that stuff.

John Marsh 11:08
Okay, um so moving on to the next topic then for the next few minutes, let's discuss your disposition to value privacy. How do you personally feel about privacy or your privacy?

11269613365 11:23
•[CNTL10]So I feel I'm in control that. So uh if I want something to be private, then I won't put it on a social media site. So I mean, there's things that you look at my social media sites, I probably, I'm guessing you probably have. There's not much out there. So it's, uh, it's pretty vanilla. And like, I try to stay away from politics or a lot of personal opinions. Most of it has to do with pictures of the family and stuff like that. •[BNFT09]So it's, it's stuff that I wouldn't mind put it on there because I want a large number of people to be able to see it, i.e., my friends, so I'm not looking for any real privacy in those settings. •[CNTL22]If I'm looking for privacy, then I'll send you know, a personal email or a letter, write someone a letter and send it.

John Marsh 12:17
All right. Just taking some notes here. Um, all right, so the next topic, for the next few minutes, let's discuss your level of concern regarding ICWATCH scraping and posting your data.

11269613365 12:32
So I saw that I'm not real sure if ICWATCH is a government thing or a commercial thing.

John Marsh 12:39
I can answer that, that they are a private entity. And right now they are being hosted by WikiLeaks.

11269613365 12:48
•[CNTL12]Okay. So once again, I mean it's, it's up to me to be careful of what I put out there in terms of uh you know what content I make available. •[PRBF15]So maybe you have a question about it, you know, we've been instructed to contact the government, if you have, if you have any concerns, so uh most of that stuff has been vetted that that I would ever talk about, I have very little out there. •[CNTL09]I mean, I have a resume that's been there forever, and it's pretty vanilla. And the government's seen it. So it's uh, you know, once again, I'm kind of careful about that. I don't go any further than that. •[CNTL20]So we

want to talk about additional data that I make sure that we talk in a space somewhere where I know that it's, it's uh been SCIF'd for the discussion that we're about to have. •[CNTL07]So once again, I thought, you know if your personal responsibility to monitor that, so I wouldn't expect uh uh a site, a social media site to be able to uh protect, I shouldn't be discussing that. •[COLL13]So I thought, I thought that was it I just wasn't real sure ICWATCH almost sounds like a government function so but I'm sure the government does the same thing with my with me too also so same thing ICWATCH. I'm guessing the government's also doing the same thing.

John Marsh 14:27
Alright, so topic four last topic. So finally let's discuss your intention to modify your LinkedIn profiles visibility.

11269613365 14:38
Okay, so uh I don't think I have anything was that

John Marsh 14:50
I was just gonna elaborate has this situation uh influenced your desire to modify the visibility of your LinkedIn profile?

11269613365 14:59
•[PRBF13]No, once again, I just it's my opinion that if I put something on a link on a link like LinkedIn so I would say something like clearancejobs.com all of them. Yeah, I mean it would I follow the rules the government has given me and that and then I would expect it to be open source anybody that looks at those sites that once again, I don't let every I don't. •[GPCN03]I don't friend everybody asked to be friended I think you asked and I did for you. But uh just because of the topic you were working on, but yeah, I mean, I don't if I don't know the person, •[USGE03]I don't know what they're doing with the data, then I'm pretty I close it down pretty, pretty uh tightly. •[CNTL21]I know everybody that's on my site. •[PRBF11]I also realize that people that know know people that I know can see my some of my stuff because they, they share it. So, once again, I uh it's my assumption that anything that's on those sites is going to be open source to anybody. •[CNTL06]So I don't I don't perceive any, any uh expectation of privacy when dealing with those sites but if I want to be private, then I'll write an email, I won't, it won't be on some kind of uh, I guess it's, you know, there's a push-pull arrangement, right? It won't be on a site where people can pull data. •[CNTL11]If I'm worried about it, it's gonna be a situation where I'll push it to the guy. And it won't be through the site, it'll be through an email or something a little bit more secure. •[PRBF23]Even when you send an email, you know, to a friend, you're not necessarily secure all the time, but that's a whole different problem where people have hacked into people's email accounts. •[BNFT08]So that to me is a social media site's all about us out there trying to basically generate a network. So that's how I use it. So probably not a very fun interview, screw you up?

John Marsh 17:15

Oh, no, no, it's perfectly fine. I'm just basically capturing your thoughts on it. So no, that's fine. Um, so I'll give you here an opportunity for any uh additional comments based on what you've discussed over those topics.

11269613365 17:29
I'm not, I want to participate because I just, I hear my uh my niece is a big uh software person. She worked at gosh can't remember the name of the company. I'm old and I'm getting senile, but she worked for [company name removed] now. And uh she gets all upset about like, Facebook and all these things. And I'm just like, are you kidding me? •[PRBF09]So it's a social media site. So anyway, and I know there's a lot, a lot of millennials, I guess there's an expectation of these things to be more than what they were intended to be, I think, so. These expectations evolve. And I don't really know what the foundation for it is why they believe that. But uh that's why I wanted to participate with this with you just because I wanted to uh. There's some personal [indecipherable word]. •[CNTL04]So people have to take a personal uh position on what they're doing, what they're posting out there. •[CNTL05]So you gotta, you kind of gotta filter what you're saying and doing and uh uh its kinda, I don't think there's any expectation. •[PRBF24]I don't have an expectation of privacy on any of those sites.

John Marsh 18:50
All right. Um, so, thank you again for your participation.

11269613365 18:55
All right

John Marsh 18:56
This concludes my data collection.

11269613365 18:58
Okay,

References

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

Ball, K., Daniel, E. M., & Stride, C. (2012). Dimensions of employee privacy: An empirical study. *Information Technology & People, 25*(4), 376-394. http://doi:10.1108/09593841211278785

Balsamo, M., & Liedtke, M. (2018, December 19). DC slaps Facebook with latest suit targeting privacy lapses. *Associated Press.* https://www.apnews.com/9cba2777340147b291c7b8604369647c

Bansal, G., & Zahedi, F. M. (2014). Trust-discount tradeoff in three contexts: Frugality moderating privacy and security concerns. *Journal of Computer Information Systems, 55*(1), 13-29. http://doi:10.1080/08874417.2014.11645737

Bansal, G., Zahedi, F. M., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems, 49*(2), 138-150. http://doi:10.1016/j.dss.2010.01.010

Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management, 53*(1), 1-21. http://doi:10.1016/j.im.2015.08.001

Benson, V., Saridakis, G., & Tennakoon, H. (2015). Information disclosure of social media users: Does control over personal information, user awareness and security notices matter? *Information, Technology & People, 28*(3), 426-441. http://doi:10.1108/ITP-10-2014-0232

Bollen, K. A. (1989). *Structural equations with latent variables.* New York: Wiley.

Chakraborty, R., Vishik, C., & Rao, H. R. (2013). Privacy preserving actions of older adults on social media: Exploring the behavior of opting out of information sharing. *Decision Support Systems, 55*(4), 948-956. http://doi:10.1016/j.dss.2013.01.004

Chen, R. (2013a). Living a private life in public social networks: An exploration of member self-disclosure. *Decision Support Systems, 55*(3), 661-668. http://doi:10.1016/j.dss.2012.12.003

Chen, R. (2013b). Member use of social networking sites - An empirical examination. *Decision Support Systems, 54*(3), 1219-1227. http://doi:10.1016/j.dss.2012.10.028

Chen, R., & Sharma, S. (2012). Understanding user behavior at social networking sites: A relational capital perspective. *Journal of Global Information Technology Management, 15*(2), 25-45. http://doi:10.1080/1097198X.2012.11082754

Chen, R., & Sharma, S. K. (2015). Learning and self-disclosure behavior on social networking sites: The case of Facebook users. *European Journal of Information Systems, 24*(1), 93-106. http://doi:10.1057/ejis.2013.31

Choi, B., & Land, L. (2016). The effects of general privacy concerns and transactional privacy concerns on Facebook apps usage. *Information & Management, 53*(7), 868-877. http://doi:10.1016/j.im.2016.02.003

Christin, D., Reinhardt, A., Kanhere, S. S., & Hollick, M. (2011). A survey on privacy in mobile participatory sensing application. *Journal of Systems and Software, 84*(11), 1928-1946. http://doi:10.1016/j.jss.2011.06.073

Cichy, P., Salge, T. O., & Kohli, R. (2014, December 15). *Extending the privacy calculus: The role of psychological ownership* [Paper presentation]. 35th International Conference on Information Systems. Auckland, New Zealand.

Claybaugh, C. C., & Haseman, W. D. (2015). Understanding professional connections in LinkedIn - A question of trust. *Journal of Computer Information Systems, 54*(1), 94-105. http://doi:10.1080/08874417.2013.11645675

Conger, S., Pratt, J. H., & Loch, K. D. (2013). Personal information privacy and emerging technologies. *Information Systems Journal, 23*(5), 401-417. http://doi:10.111/j.1365-2527.2012.00402.x

Creswell, J. W., & Plano Clark, V. L. (2018). *Designing and conducting mixed methods research* (3rd ed.). Thousand Oaks, CA: Sage.

Defense.gov (2019). Portrait of active duty women [pdf file]. https://www.defenseculture.mil/Portals/90/Documents/Research/Publications/DEMORPT-Women_Demographics-20190308.pdf

Dinev, T. (2014). Why would we care about privacy? *European Journal of Information Systems, 23*(2), 97-102. http://doi:10.1057/ejis.2014.1

Dinev, T, & Hart P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61-80. http://doi:10.1287/isre.1060.0080

Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance – An empirical investigation. *Journal of Strategic Information Systems, 17*(3), 214-233. http://doi:10.1016/j.jsis.2007.09.002

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

Farrell, P. (2016, February 2). Government monitoring social media accounts to hunt down welfare fraud. *The Guardian.* https://www.theguardian.com/australia-news/2016/feb/03/government-monitoring-social-media-accounts-to-hunt-down-welfare

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39-50. http://doi:10.1177/002224378101800104

Gefen, D., & Straub, D. W. (2005). A practical guide to factorial validity using PLS-graph: Tutorial and annotated example. *Communications of the Association for Information Systems 16*(5), 39-50. http://doi:10.17705/1CAIS.01605

Gerlach, J., Widjaja, T., & Buxmann, P. (2015). Handle with care: How online social network providers' privacy policies impact users' information sharing behavior. *Journal of Strategic Information Systems, 24*(1), 33-43. http://doi:10.1016/j.jsis.2014.09.001

Gu, J., Xu, Y., Xu, H., Zhang, C., & Ling, H. (2017). Privacy concerns for mobile app download: An elaboration likelihood model perspective. *Decision Support Systems, 94*, 19-28. http://doi:10.1016/j.dss.2016.10.002

Hong, W., & Thong, J. Y. L. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS Quarterly, 37*(1), 275-298. https://www.jstor.org/stable/43825946

Hui, K. L., Teo, H. H., & Lee, S. Y. T. (2007). The value of privacy assurance: An exploratory field experiment. *MIS Quarterly, 31*(1), 19-33. https://www.jstor.org/stable/25148779?seq=1

ICWATCH Surveillance. (2015, March 31). https://transparencytoolkit.org/project/icwatch/

Isaac, M. (2019, January 30). Facebook's profits and revenue climb as it gains more users. *New York Times.* https://www.nytimes.com/2019/01/30/technology/facebook-earnings-revenue-profit.html?searchResultPosition=1

Jarvenpaa, S. L., Tractinsky, N., & Saarinen, L. (1999). Consumer trust in an internet store: A cross-cultural validation. *Journal of Computer-Mediated Communication, 5*(2), 45-71. http://doi:10.1111/j.1083-6101.1999.tb00337.x

Jarvenpaa, S. L., Tractinsky, N., & Vitale, M. (2000). Consumer trust in an internet store. *Information Technology Management, 1*(1-2), 45-71. http://doi:10.1023/A:1019104520776

Jiang, Z., Heng, C. S., & Choi, B. C. F. (2013). Privacy concerns and privacy-protective behavior in synchronous online social interactions. *Information Systems Research, 24*(3), 579-595. http://doi:10.1287/isre.1120.0441

Joinson, A., Reips, U.-D., Buchanan, T., & Schofield, C. (2010). Privacy, trust, and self-disclosure online. *Human-Computer Interaction, 25*(1), 1-24. http://doi:10.1080/07370020903586662

Joy, W. (2016, November 15). LMPD, ACLU clash over social media surveillance. *Wave 3 News.* http://www.wave3.com/story/33720070/lmpd-and-aclu-clash-over-social-media-surveillance

Kayhan, V. O., & Davis, C. J. (2016). Situational privacy concerns and antecedent factors. *Journal of Computer Information Systems, 56*(3), 228-237. http://doi: 10.1080/08874417.2016.1153913

Kobsa, A. (2007). Privacy-enhanced personalization. *Communications of the ACM, 50*(8), 24-33. https://doi:10.1145/1278201.1278202

Ku, Y.-C., Chen, R., & Zhang, H. (2013). Why do users continue using social networking sites? An exploratory study of members in the United States and Taiwan. *Information & Management, 50*(7), 571-581. http://doi:10.1016/j.im.2013.07.011

Külcü, Ö., & Henkoğlu, T. (2014). Privacy in social networks: An analysis of Facebook. *International Journal of Information Management, 34*(6), 761-769. http://doi:10.1016/j.ijinfomgt.2014.07.006

Li, H., Gupta, A., Zhang, J., & Sarathy, R. (2014). Examining the decision to use standalone personal health record systems as a trust-enabled fair social contract. *Decision Support Systems, 57*, 376-386. http://doi:10.1016/j.dss.2012.10.043

Li, H., Luo, X., Zhang, J., & Xu, H. (2017). Resolving the privacy paradox: Toward a cognitive appraisal and emotion approach to online privacy behaviors. *Information & Management, 54*(8), 1012-1022. http://doi:10.1016/j.im.2017.02.005

Li, H., Sarathy, R., & Xu, H. (2010). Understanding situational online information disclosure as a privacy calculus. *Journal of Computer Information Systems, 51*(1), 62-71. http://doi:10.1080/08874417.2010.11645450

Li, H., Sarathy, R., & Xu, H. (2011). The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems, 51*(3), 434-445. http://doi:10.1016/j.dss.2011.01.017

Li, K., Lin, Z., & Wang, X. (2015). An empirical analysis of users' privacy disclosure behaviors on social network sites. *Information & Management, 52*(7), 882-891. http://doi:10.1016/j.im.2015.07.006

Li, T., & 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, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems*, *54*(1), 471-481. http://doi:10.1016/j.dss.2012.06.010

Li, Y. (2014). The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns. *Decision Support Systems, 57*, 343-354. http://doi:10.1016/j.dss.2013.09.018

LinkedIn. (2019). Your network and degrees of connection. https://www.linkedin.com/help/linkedin/answer/110/your-network-and-degrees-of-connection?lang=en

Luo, X., Warkentin, M., & Li, H. (2013). Understanding technology adoption trade-offs: A conjoint analysis approach. *Journal of Computer Information Systems, 53*(3), 65-74. http://doi:10.1080/08874417.2013.11645633

Mackenzie, S. B., & Spreng, R. A. (1992). How does motivation moderate the impact of central and peripheral processing on brand attitudes and intentions? *Journal of Consumer Research, 18*(4), 519-529. http://doi:10.1086/209278

Maheshwari, S., & Isaac, M. (2016, November 11). Facebook will stop some ads from targeting users by race. *New York Times.* http://www.nytimes.com/2016/11/12/business/media/facebook-will-stop-some-ads-from-targeting-users-by-race.html?_r=0

Malhotra, N., Kim, 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. http://doi:10.1287/isre.1040.0032

Mao, E., & Zhang, J. (2013). The role of privacy in the adoption of location-based services. *Journal of Information Privacy & Security, 9*(2), 40-59. http://doi:10.1080/15536548.2013.10845678

Martinez, M. J. (2016, September 29). Amazon error may end "dynamic pricing." *ABC News*. http://abcnews.go.com/Technology/story?id=119399&page=1

Miller, C. C. (2013, October 1). Google accused of wiretapping in Gmail scans. *New York Times*. http://www.nytimes.com/2013/10/02/technology/google-accused-of-wiretapping-in-gmail-scans.html

Miltgen, C. L., & Peyrat-Guillard, D. (2014). Cultural and generational influences on privacy concerns: A qualitative study in seven European countries. *European Journal of Information Systems, 23*(2), 103-125. http://doi:10.1057/ejis.2013.17

Miltgen, L. M., & Smith, H. J. (2015). Exploring information privacy regulation, risks, trust, and behavior. *Information & Management, 52*(6), 741-759. http://doi:10.1016/j.im.2015.06.006

Min, J., & Kim, B. (2015). How are people enticed to disclose personal information despite privacy concerns in social network sites? The calculus between benefit and cost. *Journal of the Association for Information Science and Technology, 66*(4), 839-857. http://doi:10.1002/asi.23206

Nunnally, J. C. (1978). *Psychometric theory* (2nd ed.). New York: McGraw-Hill.

Osatuyi, B. (2015). Personality traits and information privacy concern on social media platforms. *Journal of Computer Information Systems, 55*(4), 11-19. http://doi:10.1080/08874417.2015.11645782

Ozdemir, Z., Smith, H., & Benamati, J. (2017). Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study. *European Journal of Information Systems, 26*(6), 642-660. http://doi:10.1057/s41303-017-0056-z

Pavlou, P. A. (2011). State of the information privacy literature: Where are we now and where should we go? *MIS Quarterly, 35*(4), 977-988. http://doi-org.unr.idm.oclc.org/10.2307/41409969

[re:publica]. (2015, May 6). *re:publica 2015 - M. C. McGrath: Watching the watchers: Building a sousveillance [sic] state*. [Video File]. https://youtu.be/xipI-0HU010

Rusk, J.-D. (2014). Trust and decision making in the privacy paradox. *Proceedings of the Southern Association for Information Systems Conference, 32*, 1-6. AIS Electronic Library (AISeL). http://aisel.aisnet.org/sais2014/32

Satariano, A. (2019, January 21). Google is fined $57 million under Europe's data privacy law. *New York Times*. https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html

Schwaig, K. S., Segars, A. H., Grover, V., & Fiedler, K. D. (2013). A model of consumers' perceptions of the invasion of information privacy. *Information & Management, 50*(1), 1-12. http://doi:10.1016/j.im.2012.11.002

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly, 32*(3), 167-196. http://doi:10.2307/249477

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

Son, J.-Y., & Kim. S. S. (2008). Internet users' information privacy-protective responses: A taxonomy and a nomological model. *MIS Quarterly, 32*(3), 503-529. http://doi:10.2307/25148854

Spiekermann, S., & Cranor, L. F. (2009). Engineering privacy. *IEEE Transactions on Software Engineering, 35*(1), 67-82. http://doi:10.1109/TSE.2008.88

Stewart, K., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. *Information Systems Research, 13*(1), 36-49. http://doi:10.1287/isre.13.1.36.97

Straub, D., Limayem, M., & Karahanna-Evaristo, E. (1995). Measuring system usage: Implications for IS theory testing. *Management Science, 41*(8), 1328 -1342. http://doi:10.1287/mnsc.41.8.1328

Treiblmaier, H., & Chong, S. (2011). Trust and perceived risk of personal information as antecedents of online information disclosure: Results from three countries. *Journal of Global Information Management, 19*(4), 76-94. http://doi:10.4018/jgim.2011100104

U.S. Federal Trade Commission. (2014). *Data brokers: A call for transparency and accountability.* https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

U.S. Office of the Director of National Intelligence. (n.d.). Members of the IC. https://www.dni.gov/index.php/what-we-do/members-of-the-ic

U.S. Office of the Director of National Intelligence. (2016, May 12). Collection, use, and retention of publicly available social media information in personnel security background investigations and adjudications (Security Executive Agent Directive 5). Washington, DC. https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2016/item/1592-dni-clapper-signs-new-policy-on-social-media-for-federal-background-investigations-for-security-clearances

Wakefield, R. (2013). The influence of user affect in online information disclosure. *Journal of Strategic Information Systems, 22*(2), 157-174. http://10.1016/j.jsis.2013.01.003

Warren, S. D., & Brandeis, D. L. (1890). The right to privacy. *Harvard Law Review, 4*(5), 193-220.

Xu, H. (2010). Locus of control and location privacy: An empirical study in Singapore. *Journal of Global Information Technology Management, 13*(3), 63-87. http://10.1080/1097198X.2010.10856520

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the AIS, 12*(12), 798-824. http://doi:10.17705/1jais.00281

Xu, H., & Gupta, S. (2009). The effects of privacy concerns and personal innovativeness on potential and experienced customers' adoption of location-based services. *Electronic Markets, 19*(2-3), 137-149. http://doi:10.1007/s12525-009-0012-4

Xu, H., Luo, X., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems, 51*(1), 42-52. http://doi:10.1016/j.dss.2010.11.017

Xu, H., Teo, H.-H., Tan, B., & Agarwal, R. (2012). Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: A study of location-based services. *Information Systems Research, 23*(4), 1342-1363. http://doi:10.1287/isre.1120.0416

Zhang, R., Chen, J. Q., & Lee, C. J. (2013). Mobile commerce and consumer privacy concerns. *Journal of Computer Information Systems, 53*(4), 31-38. https://doi-org.unr.idm.oclc.org/10.1080/08874417.2013.11645648

Zhang, X., Liu, S., Chen, X., Wang, L., Gao, B., & Zhu, Q. (2018). Health information privacy concerns, antecedents, and information disclosure intention in online health communities. *Information & Management, 55*(4), 482-493. http://doi:10.1016/j.im.2017.11.003

Zhou, T. (2011). The impact of privacy concern on user adoption of location-based services. *Industrial Management & Data Systems, 111*(2), 212-226. https://doi:10.1108/02635571111115146

Zhou, T. (2015). Understanding user adoption of location-based services from a dual perspective of enablers and inhibitors. *Information Systems Frontiers, 17*(2), 413-422. http://doi:10.1007/s10796-013-9413-1