DIGITAL PRIVACY: A QUANTITATIVE STUDY EXPLORING THE INFLUENCE OF PRIVACY FATIGUE ON PRIVACY MANAGEMENT BEHAVIOR IN GENERATION Z COLLEGE STUDENTS

By

Sara Allison Brake

Liberty University

A Dissertation Presented in Partial Fulfillment

Of the Requirements for the Degree

Doctor of Philosophy

Liberty University

2022

DIGITAL PRIVACY: A QUANTITATIVE STUDY EXPLORING THE INFLUENCE OF PRIVACY FATIGUE ON PRIVACY MANAGEMENT BEHAVIOR IN GENERATION Z COLLEGE STUDENTS

By Sara Allison Brake

A Dissertation Presented in Partial Fulfillment
Of the Requirements for the Degree
Doctor of Philosophy

Liberty University, Lynchburg, VA
2022

APPROVED BY:

Tabitha L. Cassidy, PhD, Committee Chair

Wesley Hartley, PhD, Committee Member

Robert K. Mott, PhD, Online Program Chair

ABSTRACT

Generation Z has grown up in a digital environment where their physical world is often merged with their digital world. Research has found that students often blindly accept social media terms and agreements because they feel they have no choice. Therefore, many students are often lacking in knowledge regarding privacy protection behavior on social media platforms. Some scholars argue that this creates a privacy paradox, while others argue it elicits privacy fatigue. In addition, there is little centralized regulation for online privacy, and privacy agreements vary by social media platform. The purpose of this study was to explore the variables of privacy fatigue, privacy concern, privacy control, and privacy management and their impact on Generation Z college students' behavior within the framework of communication privacy management theory. A quantitative research method with a 7-point Likert-type survey was used to assess the attitudes of Generation Z college students between the ages of 18-25. The results found that privacy control and privacy concern were predictors of privacy fatigue. When students feel less control over their personal information online, their level of privacy fatigue increases. This study has theoretical implications within communication privacy management theory. The study also has practical implications for organizations and social media platforms that seek to encourage communication and interaction within their websites and apps.

Keywords: digital privacy, privacy fatigue, communication privacy management, Generation Z

Copyright Page

Table of Contents

ABSTRACT 3

List of Tables 7

List of Figures 8

CHAPTER ONE: INTRODUCTION 9

Overview 9

Background 9

Problem Statement 11

Purpose Statement 13

Significance of the Study 14

Research Question and Hypotheses 14

Definition of Terms 15

Summary 17

CHAPTER TWO: LITERATURE REVIEW 18

Overview 18

Theoretical Framework 18

Digital Privacy Background Literature 28

Summary 46

CHAPTER THREE: METHODS 48

Overview 48

Method and Design 48

Research Question and Hypotheses 50

Participants and Setting 51

Instrumentation 55

Procedures 56

Data Analysis 56

Summary 59

CHAPTER FOUR: RESULTS 60

Overview 60

Research Question and Hypotheses 60

Reliability and Descriptive Statistics 61

Results 67

Summary 81

CHAPTER FIVE: CONCLUSIONS 83

Overview 83

Discussion 84

Implications 91

Recommendations for Future Research 96

Conclusion 98

REFERENCES 100

APPENDIX 117

List of Tables

Table 1: *Sociodemographic of Participants* 54

Table 2: *Descriptive Statistics of Study Variables* 62

Table 3: *Reliability Statistics: Fatigue Variable* 63

Table 4: *Descriptive Statistics: Fatigue Construct*..........63

Table 5: *Reliability Statistics: Concern Variable*..........64

Table 6: *Inter-Item Correlations: Concern Variable*..........64

Table 7: *Descriptive Statistics: Concern Construct*..........65

Table 8: *Reliability Statistics: Control Variable* 65

Table 9: *Descriptive Statistics: Control Construct*..........66

Table 10: *Reliability Statistics: Management Variable*..........66

Table 11: *Descriptive Statistics: Management Construct* 67

Table 12: *Correlations* 72

Table 13: *Variance Inflation Factors for Concern, Management and Control*..........76

Table 14: *Model Summary* 77

Table 13: *Coefficients* 78

Table 14: *Group Statistics* 79

Table 15: *Independent Samples Test*..........80

Table 16: *Group Statistics* 81

Table 17: *Independent Samples Test* 81

List of Figures

Figure 1: *Male and Female Respondents* 52

Figure 2: *Preferred Device and Platform* 52

Figure 3: *Scatterplots for Concern and Management, Concern and Fatigue* 69

Figure 4. *Scatterplots for Concern and Control, Management and Fatigue* 69

Figure 5: *Scatterplots for Management and Control, Fatigue and Control* 70

Figure 6: *Homoscedasticity for Linear Regression* 73

Figure 7: *P-P scatterplot for normality: Fatigue* 74

Figure 8: *P-P scatterplot for normality: Concern* 74

Figure 9: *P-P scatterplot for normality: Control* 75

Figure 10: *P-P scatterplot for normality: Management* 75

Figure 11: *Privacy Fatigue Scales*..93

Figure 12: *Privacy Management Scales* 95

CHAPTER ONE: INTRODUCTION

Overview

The concept of privacy is not new to modern society and the information age. Westin (1970) described privacy as “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others” (p. 7). In 1966, the International Covenant on Civil and Political Rights by the United Nations established privacy as a human right, stating everyone has a right to privacy (Office of the United Nations High Commissioner for Human Rights, 1966). With the advancement of digital technology, the United Nations has addressed the right to digital privacy, declaring that the rights people are afforded offline should also be protected online (OHCHR, n.d.). In April 2015, the Human Rights Council adopted a resolution that appointed an independent expert to report on digital privacy violations and raise awareness of digital privacy issues (OHCHR, n.d.). The goal of the Human Rights Council is to encourage countries to create laws to protect the digital privacy of citizens. Until laws catch up with technology, users must take ownership of their digital privacy and become digitally literate in privacy protection behavior.

Background

Digital privacy is a growing issue that governments and organizations have been slow to address. Because technology changes so rapidly, lawmakers struggle with figuring out how to enforce digital privacy protection (Boerman et al., 2018). In a survey on digital privacy, 84% of Americans stated that they felt they had little to no control over the data collected by the government, while 81% felt they had little to no control of data collected by organizations (Pew Research Center, 2019). While Europe has taken action to improve privacy protection with the General Data Protection Regulation (GDPR), in most of the United States, consumers are left to take ownership of protecting their digital privacy. Unfortunately, most consumers do not have the digital literacy to adequately protect their online data. Privacy settings on websites or social media platforms often give consumers a false sense of security (Jozani et al., 2020). It can be argued that without laws and regulations that oversee a company's collection and use of consumers' private data, consumers are at the mercy of large corporations when it comes to protecting their digital privacy. The first state privacy law, California Consumer Privacy Act (CCPA), was passed in June 2018 and gives California consumers the right to see data that a company has saved on them as well as sue a company for privacy violations (Korolov, 2020). The companies do not have to be based in California or even the United States to fall under the law which began to be enforced on July 1, 2020 (Korolov, 2020). However, it is important to note that California is the location for many large data corporations such as Google, Facebook, and Apple. CCPA is seen as one of the first steps leading to either U.S. federal privacy regulation or other state privacy laws (Baik, 2020).

Apple is taking steps to protect users' digital privacy by allowing users to choose whether or not apps can track their information. This software change has upset Facebook because the social media platform relies on users' data to provide targeted marketing to advertisers. Facebook has accused Apple of making this move not for privacy but for profit. Apple controls half of the smartphone market in the United States with more than 1 billion iPhone users (Kim, 2021). Not only will Apple's apparent support for users' digital privacy have the potential to increase sales, but it may also increase app costs and purchases, which Apple directly benefits from monetarily (Kim, 2021). However, Apple appears to be taking steps to give users more control of their privacy and data. Knowing that they possess some control over their private information, people feel less vulnerable (Petronio & Child, 2020).

Facebook is also facing challenges in Europe with its messaging app, WhatsApp. The European Consumer Organisation (BEUC) has filed a complaint against WhatsApp for harassing users with pop-up messages that state users must accept the new terms of use and privacy policy or lose access to the app (Hart, 2021). BEUC argued that the language of the policy is complicated, and users are unable to understand the new terms of agreement (Hart, 2021). This is also occurring in the United States but with less public and government resistance. Users have been given no choice but to accept the new terms and privacy policy or lose their ability to use the app. This puts consumers in a losing situation. It also creates what researchers have termed privacy fatigue (Choi et al., 2018; Tang et al., 2020). Worn down by an overflow of information and confusing terms, users feel there is no way to effectively manage their digital privacy.

Problem Statement

Digital privacy has been described as what people "conceal and reveal" and "what others acquire and ignore" (Anthony et al., 2017, p. 251). Privacy management is crucial to social order, creating a balance of what is revealed and concealed (Anthony et al., 2017). General day-to-day privacy management is difficult on its own; digital technology creates new privacy challenges that can be overwhelming. With the rapid advancement of technology, data privacy legislation and other privacy regulations have not kept pace with digital technology and how companies collect personal data online. Learning how to navigate the terms and agreements on websites and utilizing privacy settings can be a daunting task. This is especially true for college students who may be managing their online identity on their own for the first time without parental or school support. Therefore, it is critical for college students to take ownership of their privacy and the protection of their online data (Boerman et al., 2018). For Generation Z, the digital generation, maintaining an online presence and identity is important to their social culture and communication (Marron, 2015; Rospigliosi, 2019). However, the general problem is that few studies have investigated Generation Z's privacy protection behavior and their concern for digital privacy.

Media often portray teens and college students as reckless with no care for online privacy (Benjamin, 2017). However, researchers have found that some Generation Z students are concerned with digital privacy and that they do employ some privacy protection behavior, but they may not have the digital literacy required to effectively protect their data (Hargittai & Marwick, 2016). Some researchers described this behavior as the privacy paradox (Hargittai & Marwick, 2016), while others argued that students could be experiencing privacy fatigue (De Wolf, 2020). It has been argued that privacy fatigue better describes the privacy protection of teens and young adults rather than the privacy paradox; however, further research is needed (Choi et al., 2018; De Wolf, 2020).

As previously noted, Generation Z is known as the digital generation, having grown up immersed in digital technology (Marron, 2015; Rospigliosi, 2019). Marron (2015) coined the term "screenagers" to describe Generation Z because they are considered the most technologically connected generation to date (p. 124). Generation Z prefers to receive information digitally and quickly, even finding traditional email lacking in quickness and ease of use (Beck & Wright, 2019). This digital generation prefers texts, social media, and other apps for communication, social interaction, and even education (Beck & Wright, 2019). According to Marron (2015), this use of technology has given Generation Z the ability to learn in various settings. Research that specifically explores the relationship between online privacy protection behavior and privacy fatigue has not been studied in the Generation Z college student demographic.

De Wolf (2020) conducted a study examining teens' digital privacy behavior using communication privacy management theory as a framework. He highlighted the work of Choi et al. (2018), who related privacy fatigue to the privacy paradox in online privacy disclosure behavior. De Wolf’s study highlighted CPM theory’s failure to address privacy fatigue as it relates to online privacy management. The problem is that little is known about how privacy fatigue impacts the privacy management behavior of Generation Z and their online communication. Recent studies, such as those by De Wolf (2020) and Choi et al. (2018), suggested that further exploration is needed on privacy fatigue as it relates to privacy concern within the CPM framework. It is also suggested that CPM theory should be further studied and adapted for digital communication (De Wolf, 2020).

This research study added to the scholarly research on digital privacy, privacy fatigue, and CPM theory. Additionally, it focused on Generation Z, the digital generation. While there has been a great deal of research on previous generations, very few studies have explored the digital communication trends of Generation Z. This study attempted to fill the gap in research about Generation Z and digital privacy, particularly as it relates to CPM theory and privacy fatigue.

Purpose Statement

The purpose of this study was to explore how privacy fatigue impacts the digital privacy protection behavior of Generation Z and to test communication privacy management (CPM) theory. The variables in the study included privacy fatigue, privacy concern, privacy control, and privacy management. CPM theory acknowledges that people own their private information and control access to that information, which is regulated through privacy boundaries (Petronio & Child, 2020). The study was limited by the age and education of participants. Additionally, the study utilized a cross-sectional survey in which data was collected online. Online surveys are convenient and cost-effective. Furthermore, as Gen Z is the digital generation, digital communication is the preferred medium.

Significance of the Study

To date, no study has specifically examined the influence of privacy fatigue on the digital privacy management behavior of Generation Z college students. This study sought to contribute new privacy fatigue research within the framework of CPM theory. Because communicating in a digital environment cannot feasibly be avoided, students must learn how to effectively manage their personal privacy online and reduce inevitable privacy turbulence. By studying the impact of privacy fatigue, this research aimed to provide a further understanding of Generation Z's online communication and boundary management. Additionally, by establishing a connection between privacy fatigue, privacy concern, privacy control, and privacy management, this research provided insights into how organizations can provide better privacy practices and encourage safe and effective online communication.

Research Question and Hypotheses

In their study exploring online privacy behavior, Choi et al. (2018) found that privacy fatigue had a more significant impact on privacy behavior than privacy concerns. While many variables impact an individual's privacy protection behavior, privacy concern is one of the major factors studied in most online privacy behavior research. As of this writing, Choi et al. is the only study that has compared privacy concern and privacy fatigue. Furthermore, there has been no research examining the impact of privacy fatigue on the privacy protection behavior of Generation Z college students. Therefore, this study sought to build on previous privacy fatigue research by asking the following research question and hypotheses:

RQ 1: Does communication privacy management theory explain the relationship between privacy fatigue and privacy concern in Generation Z college students?

H1: Generation Z college students that exhibit a higher level of privacy concern will feel a higher level of privacy fatigue.

H2: Generation Z college students that exhibit a higher level of privacy concern feel less control over their online privacy.

H3: Generation Z college students who express a higher level of privacy concern will utilize more privacy management strategies on social media.

H4: Generation Z college students with a higher level of privacy fatigue will feel they have less control over their online privacy.

H5: Generation Z college students with a higher level of privacy fatigue will employ less online privacy management strategies.

H6: Generation Z college students who utilize more privacy management strategies will feel more control over their privacy on social media.

H7: Female Generation Z college students exhibit more privacy concern and privacy fatigue than male Generation Z college students.

Definition of Terms

Terms can have varying meanings depending on the author and context. Therefore, the following section defines how key terms are used throughout the study.

- **digital privacy**: Privacy can be difficult to define because it means different things to different people. For the purpose of this study, digital privacy refers to the protection of personal information that is disclosed online or within a digital environment (Becker, 2019; Hunter & Taylor, 2020).

- **privacy fatigue:** As defined by Choi et al. (2018), privacy fatigue describes the weariness that users experience when they feel that there is no effective way to manage personal information in a digital environment.
- **Generation Z:** For the purpose of this study, Generation Z is considered to be people who were born between the years 1996-2010 (Dimock, 2019). The age group within Generation Z that this study specifically researched are those between the ages of 18-25.
- **privacy paradox**: The term "privacy paradox" is defined as the behavior exhibited by users who state they are concerned about their digital privacy, but their sharing and disclosure behavior online suggests differently (Hargittai & Marwick, 2016).
- **privacy protection behavior**: For the purpose of this study, the term privacy protection behavior is defined as the actions a person takes to protect their digital data. For example, these actions may include blocking people or information, using pseudonyms, using different social media platforms for different purposes, and using privacy settings within a social media platform (Wisniewski et al., 2017).
- **digital privacy and literacy**: The term digital literacy is used to describe the knowledge students require to critically evaluate and communicate within digital media, particularly in how it relates to data privacy (Park, 2011). Privacy literacy is defined by Trepte et al. (2015) as "users' ability to apply strategies for individual privacy regulation and data protection" (p 339). Additionally, it refers to possessing online privacy knowledge regarding current technology and data protection laws (Trepte et al., 2015).
- **privacy turbulence**: The term privacy turbulence was coined by Petronio as a factor in communication privacy management theory (Petronio & Child, 2020). For the purpose of this study, privacy turbulence will be used to describe the unexpected privacy violations

students encounter when sharing information online. Becker (2019) stated a privacy violation is “a violation of or intrusion into something valuable that should be protected” (p. 307).

Summary

This chapter introduced the background of digital privacy as well as the purpose of the study. It discussed privacy as a human right and the significance of online privacy protection behavior and Generation Z. Specifically, the chapter focused on privacy fatigue and its potential impact on privacy behavior. The following chapter will present a review of current literature describing digital privacy, the privacy paradox, digital literacy, and privacy fatigue. Additionally, it provides the background for the theoretical construct of the study, communication privacy management theory, as well as the gaps in privacy fatigue research. Chapters Three, Four, and Five will present the methodology, results, discussion, and conclusion.

CHAPTER TWO: LITERATURE REVIEW

Overview

Privacy is a term that is difficult to define, particularly in today's digital environment. In general, the concept of privacy is built upon the definition provided by Warren and Brandeis (1890) as "the right to be let alone" (p. 193). Anthony et al. (2017) defined digital privacy as "the access of one actor (individual, group, or organization) to another" which means that "privacy refers to what people conceal and reveal and what others acquire and ignore" (p. 251). People have taken ownership of their personal privacy, yet they often still feel that they must compromise privacy online (Hargittai & Marwick, 2016). As noted by Benjamin (2017), "While technology cannot necessarily produce a positive culture of privacy, it can at least strive not to harm it" (p. 57). When the burden of protecting privacy falls on the user, it makes data privacy even more challenging (Benjamin, 2017). College students are particularly vulnerable because they are ardent users of digital media but may not have the digital literacy skills needed to manage digital privacy boundaries. To better understand the online privacy protection behavior of Generation Z college students, this literature review will focus on digital privacy, digital literacy, and privacy fatigue within the theoretical framework of communication privacy management theory.

Theoretical Framework

The research in this study tested communication privacy management (CPM) theory and the relationship of privacy fatigue in the online privacy protection behavior of Generation Z college students. CPM theory and the study of online privacy protection behavior fall within the sociopsychological tradition of Craig's (1999) seven traditions of communication. The following section describes the research and theories that ground this study in the field of communication.

Communication Traditions

Craig sought to categorize traditions within the communication field to give a platform for debate amongst communication scholars (Jan, et al., 2017). Communication theories have been heavily influenced by other disciplines; therefore, Craig's traditions provided a more cohesive forum for communication theory (Craig, 1999; Jan et al., 2017). Craig (2008) argued that, over the years, communication has transformed into an academic discipline that provides an "intellectual coherence" to communication but is still lacking in core theories found within traditional disciplines (p. 16). He further noted that communication is a practical discipline, but it requires more than practicality to be an academic discipline. Communication as a discipline must produce research with a disciplinary perspective through communication theory. Craig's (1999) seven communication traditions aid scholars in producing communication research within disciplinary boundaries.

This research study falls within Craig's (1999) sociopsychological tradition of communication. Craig described the sociopsychological tradition of communication as "the process by which individuals interact and influence each other" (p. 143). Additionally, he noted that "communication may occur face-to-face or through technological media" (p. 143). In the sociopsychological tradition, communication behavior is influenced by a person's values, beliefs, and attitudes (Craig, 1999). It also recognizes that people are logical and practical in decision-making and seeks to provide scientific evidence for human behavior (Craig, 1999).

According to Krauss and Fussell (1996), "Social psychology traditionally has been defined as the study of the ways in which people affect, and are affected by, others" (p. 3). They also argued that communication has not always been at the center of the study of social psychology because of the multidisciplinary aspect of communication. Craig (1999) noted that social psychology “implies a strong moral imperative that we as individual communicators should make responsible choices based on scientific evidence concerning the likely consequences of our messages” (p. 144). He has taken social psychology and given it a prominent space within the communication field. CPM theory demonstrates Craig’s sociopsychological tradition.

CPM theory explores how human interaction, judgments, and beliefs impact the privacy protection behavior and boundary-setting actions of people in both offline and online settings (Petronio, 2002). It explores the cause-and-effect relationship of setting boundaries and the turbulence that happens when boundaries are broken. CPM theory provides a way to explain the sociopsychological view within the resulting consequences of communication as described by Craig (1999). Communication boundaries online are influenced not only by personal values and beliefs but also the social context within the platform. Craig (1999) stated that the sociopsychological tradition explains how communication is manipulated and influenced to produce the desired outcome. This can be found in an online environment where privacy management behavior is utilized to manipulate communication and protect personal privacy.

Communication Theory

Communication privacy management (CPM) theory was developed by Sandra Petronio (2002) in the early 1990s. At the time, it was used to describe a person’s disclosure behavior in an interpersonal, face-to-face communication setting. For example, Petronio (1994) explored the invasion of college-aged children’s privacy by their parents and how the parent-child relationship is managed. CPM theory has more recently been used to investigate users’ disclosure behavior on social media and the disclosure of digital health information and communication (Petronio, 2013). In a more recent study, Xie and Karan (2019) examined how college students created privacy boundaries for their personal information to block companies from accessing certain personal information on social media.

CPM theory describes how people determine what is to be kept private versus what is shared publicly. CPM theory involves three principles: privacy ownership, privacy control, and privacy turbulence (Petronio, 2013). It argues that people weigh the benefits of a privacy risk when determining what should be shared publicly. In 2013, Petronio discussed how CPM theory had been streamlined to make it more accessible. She stated that "privacy ownership (boundaries of private information), privacy control (privacy management engine), and privacy turbulence (privacy regulation breakdowns) are the ingredients to allow for understanding how people regulate private information" (p. 8). According to CPM theory, people take ownership of their privacy and protecting their personal information (Petronio & Child, 2020). The privacy of personal information is controlled by privacy boundaries. The term privacy turbulence is used to describe when a person's privacy has been violated or there has been a breakdown in privacy boundaries (Petronio & Child, 2020). Successfully managing privacy boundaries and privacy turbulence is important in developing social relationships.

Overview and History

CPM theory was originally called communication boundary management in Petronio's (1991) first published study of the theoretical framework. In 1994, Petronio applied it to the privacy boundaries of college-aged children and their relationships with their parents. However, Petronio (2002) stated that the theory was years in the making before these particular studies. One theory she considered as she researched was Altman and Taylor's (1973) social penetration theory. Social penetration theory analyzes social relationships as they progress from strangers to close friends (Altman & Taylor, 1973). Petronio (2002) noted that social penetration theory was not applied to disclosure research at that time. However, Altman's (1975) research on privacy management and the concept of a private space caught her attention, which aided Petronio in narrowing in on self-disclosure and privacy. In the 1980s, Petronio and Martin (1986) published a study exploring the gender gap in revealing private information. This led Petronio to focus on two aspects of disclosure for CPM theory: the content and the process. Petronio's (2002) conceptual development of information disclosure involved the private information people disclosed and the process, which is how the private information is disclosed. The more she researched and developed CPM theory, the more she found connections between privacy and disclosure as well as the contradictions and tensions they caused.

For the next decade, Petronio (2002) worked to further develop and define CPM theory. Initially called communication boundary management theory, Petronio found it necessary to change the name to one that was more descriptive and precise. The name change reduced confusion among other boundary research and family studies. Petronio outlined the framework and underlying assumptions of the theory in her 2002 book, *Boundaries of Privacy: Dialectics of Disclosure*. Petronio (2002) noted that while the theory now sounds simplistic and obvious, it is because it has been refined and researched extensively over the years.

Current CPM Theory Research

The development of digital communication has presented many challenges for CPM theory. Petronio (2013) and others have researched privacy management as it pertains to blogging (Child et al., 2011), Facebook (Waters & Ackerman, 2011), and online dating among others (Gibbs et al., 2011). To make CPM theory more accessible, Petronio streamlined the main components of the theory: privacy control, privacy ownership, and privacy turbulence. She described privacy control as the engine, privacy ownership as the boundaries, and privacy turbulence as the breakdowns.

The first component, privacy ownership, predicts that people believe they own their private information and have a right to protect that information. It also predicts that people can restrict or share that ownership (Petronio, 2013). When the information is shared, a co-ownership is created. Research has been conducted studying the impact of group or co-ownership of private information, such as in families or groups (De Wolf et al., 2014). Petronio (2013) argued that research into co-ownership has helped CPM theory be more applicable to privacy and relationships. Recently, Zhu and Kanjanamekanant (2021) studied the concept of co-ownership within CPM theory as it pertains to personalized advertising on social media platforms. They found that when users have a perception of co-ownership with a social media platform such as Facebook, they have fewer privacy concerns. Developing and maintaining appropriate boundaries promotes a relationship of co-ownership with social media platforms (Zhu & Kanjanamekanant, 2021).

The second component of the framework, privacy control, predicts that people believe they own the right to control their private information because they believe they own the right to their private information—even if there is co-ownership (Petronio, 2013). The way people control their privacy is through privacy rules. When there is co-ownership of the information, privacy rules are negotiated with the co-owners. When sharing information, particularly online, people control their privacy by revealing some information and concealing details that they feel uncomfortable sharing with a larger group (Petronio, 2013). Thus, privacy control predicts that privacy is regulated by decisions made about personal privacy boundaries. Privacy control has been frequently studied. For example, Yang and Kang (2015) found that the more users believe they have control over their private information, the more they will utilize social media.

The final component, privacy turbulence, predicts that regulating personal privacy is unpredictable and that breakdowns in privacy boundaries will happen (Petronio, 2013). Research into this particular component has increased over the years as researchers seek to understand why a privacy breach has occurred (Petronio, 2013). Petronio (2013) noted that privacy turbulence represents the need for change in privacy rules and regulations. Privacy turbulence research explores why a privacy regulation system failed and how to improve privacy management. Current research on privacy turbulence is highlighted in further detail below.

CPM Theory and Digital Privacy

Almost 20 years ago, Petronio (2002) noted that technology was having a major impact on personal privacy. In a digital environment, CPM theory seeks to explore and explain how people establish privacy rules and boundaries as well as how people manage privacy turbulence. Baruh et al. (2017) studied CPM theory along with the privacy paradox in relation to privacy management and privacy literacy on social media. They noted that privacy management is a way of controlling privacy boundaries, and privacy literacy plays an important role in influencing privacy management. Their findings suggested that users' privacy concerns do predict their privacy management behavior as well as their use of online platforms. Baruh et al. (2017) proposed that CPM theory explains how users utilize a risk-benefit analysis. Additionally, their findings that users with higher privacy literacy utilize more privacy protection behavior aligned with CPM theory's predictions of privacy rules and boundaries.

Metzger (2007) noted that CPM theory provides a good building block for examining privacy boundaries online. However, she argued that there are some fundamental differences between face-to-face communication and online communication. Therefore, CPM theory must be adapted for online communication. For example, Metzger posited that there is no evidence that online privacy boundaries are formed the same way in which privacy boundaries are formed in offline communication. She observed disparate boundaries in gender and suggested that differences in privacy boundaries online versus offline for gender vary because online disclosure behavior appear to be different than offline disclosure behavior reported in previous research. Her findings supported the boundary management strategies that CPM theory predicts. In an e-commerce setting, Metzger felt that the disclosure of information is more impersonal and less emotional than a face-to-face encounter. When applying CPM theory to group and individual privacy management on Facebook, De Wolf et al. (2014) also found differences in privacy protection behavior between genders. Women exhibited more privacy protection as individuals, while men were more likely to exhibit group privacy protection behavior. Additionally, De Wolf et al. noted that young adults and older youth were more likely to employ privacy protection behavior than younger teens. Comparing privacy protection behavior between genders provides a unique insight, while exploring various age groups may explain the impact of digital privacy literacy on privacy disclosures.

In a recent study, CPM theory was used to study the privacy concerns and social media use between generations. Nuzulita and Subriadi (2019) conducted a study in Indonesia and found that there were different perceived benefits between generations. For example, Generation Z respondents stated that they utilize social media to develop new relationships and networks with people they have never met as well as to shape their online image. While Generation Y utilized social media for relationships and networking, they also utilized it for promoting their businesses and contacting business associates. Additionally, Nuzulita and Subriadi found that the benefits of social media outweigh the risks for most people; however, privacy awareness does affect what people share, on which platform, and with whom they share. Their findings addressed certain benefits and risks noted by CPM theory, such as social control, relationship development, security risk, and relational risk. Users believed that there are privacy risks on social media, but they can be avoided with the right privacy management tools (Nuzulita & Subriadi, 2019). However, the researchers noted that CPM theory does not address other benefits of social media such as financial gain, entertainment, and information seeking.

In recent years, many other studies have been conducted on digital privacy within the framework of CPM theory. Jin (2013) explored the privacy management of Twitter users, finding that most users had layers to the amount of information disclosed on the platform. As predicted by CPM theory, people created rules and boundaries about what they reveal and conceal online (Jin, 2013). Frampton and Child (2013) used CPM theory to examine how coworker relationships cross over into the digital and social media world. They considered how working professionals manage their privacy on Facebook when a coworker sends a friend request, finding that a friend request does not create a privacy dilemma for most coworkers. This may be because research has found that most social media users continually manage their privacy boundaries and make risk-benefit calculations as predicted by CPM theory (Petronio, 2002; Petronio & Child, 2011). De Wolf et al. (2014) and De Wolf (2020) also explored privacy management on social media within the framework of CPM theory. In CPM theory digital privacy research, privacy turbulence played a role in motivating users to adjust their privacy management strategy.

Privacy Turbulence Online

Privacy turbulence can happen when someone intentionally violates a privacy boundary, when a boundary is not clear, or when there is a privacy dilemma (Petronio, 2002). Petronio (2002) stated, “We may encounter minor flare-ups, confusion, misunderstandings, mistakes, embarrassments, and full-fledged uproars” (p. 177). Six factors lead to boundary turbulence outlined by Petronio (2002): intentional rule violations, boundary rule mistakes, fuzzy boundaries, dissimilar boundary orientations, boundary definitions predicaments, and privacy dilemmas (p. 177). In all turbulence, a lack of effective communication is present.

Turbulence has an impact on personal relationships. When a privacy breach creates turbulence, it causes people to adjust their privacy boundaries (Petronio & Child, 2020; Trepte, 2015). When turbulence happens on social media, it is more challenging to manage. Trepte (2015) argued that managing privacy and turbulence on social media requires negotiation within users’ online network and negotiation with the social media platform by adjusting privacy settings. He further argued that turbulence on social media forces communication between networks about privacy and boundaries. Setting boundaries online is difficult due to the public nature of social media and the blurring lines of what is public versus what is private on the Internet (Barnes, 2006; Trepte, 2015). For example, Litt and Hargittai (2014) suggested that turbulence is most often caused by others rather than by a user personally over-sharing. A user may be effective in protecting their personal information, but that information may then be revealed by someone in their network, resulting in privacy turbulence. Thus, there is a need for users to negotiate boundaries within their network (Trepte, 2015).

DeGroot and Vik (2017) studied CPM theory and privacy turbulence in an online setting, finding many instances of privacy violations or turbulence could be avoided with the implementation of privacy rules. They found that people who revealed confidential information of friends and acquaintances online were not given clear privacy rules. Users disclosed information without first considering the emotional impact on the friend or acquaintance. Therefore, DeGroot and Vik argued that privacy turbulence resulted from a lack of privacy boundary rules. They also noted that there is no clear set of rules for privacy disclosure. This must be determined and clearly communicated by the owner of the information. Finally, they noted that when turbulence does occur, it changes the way users communicate and share on social media. While some current research seems to indicate that privacy turbulence is inevitable, other research supports the idea that privacy turbulence can be reduced or effectively managed by using privacy protection strategies.

Digital Privacy Background Literature

Today's society lives online with a constant digital presence from reading the news to connecting with family and friends. Large organizations, such as Google and Facebook, control a vast amount of data that people share online. This data is used to track a person's habits and location as well as purchasing and browsing history; every action online can be traced. Once information is online, it is difficult to erase, as it can be copied, shared, and saved by anyone who sees it—leaving a digital footprint. This is what Betkier (2019) calls a data subject. He noted, "Personal data can create a detailed picture of who they are, what they have been doing, with whom, what they have seen or told and what they are looking for" (p. 1). Companies sell users' personal data for targeted advertising and other marketing analytics (Betkier, 2019). In his study, Betkier (2019) argued that, when users are influenced by targeted advertisements, their social interactions and buying habits are shaped by certain characteristics, while other ideas may be stifled. Additionally, Hunter and Taylor (2020) suggested that marketers can use collected data to influence consumers' privacy and disclosure behavior on social media. Withdrawing from online participation or the consumer marketplace is not a feasible option in today's digital society; therefore, digital privacy has become a critical aspect of everyone's life (Baruh & Popescu, 2017). Digital privacy issues have a direct impact on social culture and society's function (Anthony et al., 2017; Betkier, 2019). Aside from the previously mentioned California law, there is currently little legal regulation in the United States for online privacy because lawmakers struggle with how to enforce digital privacy protection as well as keep up with rapid technological changes (Boerman et al., 2018).

When users create a profile on social media, mobile apps, or other websites, they are typically asked to agree to the site's terms and conditions. However, most users do not read these long legal documents or understand them (Baruh & Popescu, 2017). Users feel they have no choice but to accept the terms to gain access to the platform; therefore, they do not attempt to read the long legal jargon (Gerber et al., 2018). With online purchases, 59% of consumers stated that they skimmed over the terms before making a purchase, while 14% did not read the terms at all (Gerber et al., 2018). Even though some users may be concerned about their privacy, they blindly accept the terms and conditions of websites and social media apps, and this creates what researchers call the privacy paradox—a discrepancy between users' privacy concerns and online disclosure behavior discussed in the following section.

Having complete control over personal data and privacy online is not possible due to the rapid flow of digital information. Masur (2019) noted that privacy is not managed by an individual's decisions. He stated, "Establishing a certain level of privacy rather depends on collective measures, technical mechanisms, and established social norms" (p. 123). He further noted that young adults see privacy management as "more collaborative than individual" (p.

123). Therefore, Marwick and Boyd (2014) argued digital privacy management relies on social norms and trusting social relationships. Digital privacy must be viewed as not an individual management process but as something that is managed between relationships and networks (De Wolf et al., 2014; Marwick & Boyd, 2014).

Because users have expressed a lack of empowerment and control over their personal data, websites and social media platforms can provide certain conditions to empower users. Bandara et al. (2020) defined privacy empowerment as "an individual's perception of the extent to which they can produce desired outcomes and prevent undesired outcomes related to the use of their information" (p. 428). They further noted that people need the following to feel empowerment: "having control, autonomy, critical awareness, and privacy efficacy" (p. 428). However, Obar (2019) argued that there is a "fallacy of data privacy self-management" where users presume that they can self-manage and control digital privacy (p. 37). In reality, users have been placed in an impossible situation where they must attempt to manage personal data privacy on corporate-controlled platforms and with a government that has provided little regulation. Often, users have little control, particularly when it comes to privacy breaches (Yerby et al., 2019). Recent research suggests that a lack of control produces privacy concerns (Mosteller & Poddar, 2017; Punj, 2019).

In their research on digital privacy concerns, Masur and Trepte (2020) found that privacy breaches and other online experiences may increase concern but may not change privacy behavior. It is noted that people may not change their privacy protection behavior because they feel that they do not have the ability to effectively protect their privacy anyway. The researchers highlighted the gap in privacy theories, stating the theories often assume that "people's privacy behavior is based on rational decision-making" (p. 20). Instead, people may simply assume that privacy violations are inevitable. Some research has suggested that websites' lack of choices in privacy protection creates the attitude of apathy seen in the privacy paradox (Baruh & Popescu, 2017).

Privacy Paradox and Privacy Calculus

The term privacy paradox was first coined by Barnes (2006) in her research on teens' disclosure behavior on social media platforms. The privacy paradox describes the disconnect between users' privacy concerns and their actual online disclosure behavior (Barnes, 2006; Gerber et al., 2018). Users stated that they are concerned about their privacy online; however, they continue to share personal information with websites and apps, creating the privacy paradox (Gerber et al., 2018). One way that Gerber et al. (2018) explained the privacy paradox is through a privacy calculus model where users trade privacy for something that is beneficial and exceeds the risk of sharing. Users do not always know what the specific risks and benefits might be. Dienlin and Metzger (2016) observed that users "rely on past experience, intuition, or perception to assess them" (p. 370). Dienlin and Metzger supported the results of past studies on the privacy calculus. When users view benefits as higher than the potential risks, disclosure behavior is more likely to take place (Dienlin & Metzger, 2016).

The privacy calculus model is used to explain the privacy paradox in digital communication. To examine the privacy paradox within the privacy calculus model, Chen (2018) studied the impact of social capital on social media use. Chen described social capital as a strong influence on social media activity but found that social capital does not affect privacy protection behavior. Instead, social capital "can promote the positive effect of self-efficacy on protection practices" (Chen, 2018, p. 1409). Similarly, research by Trepte et al. (2020) further supported the argument that social support influences users' disclosure behavior. When users viewed other users sharing and disclosing personal information, they were more likely to disclose more information than those who did not view information disclosure. Therefore, Trepte et al. argued that “context matters” when it comes to how and why users disclose information online. When users have social support and shared interests among their network, they feel that it is worth the privacy risk to disclose information to form a stronger network or more relationships, producing the risk and benefit analysis of the privacy calculus (Trepte et al., 2020). This type of risk versus reward relationship is outlined in CPM theory.

In their 2017 study, Hallam and Zanella found that the privacy paradox still applies to self-disclosure behavior. Consequently, social rewards are connected to self-disclosure, while more abstract risks are not connected to self-disclosure (Hallam & Zanella, 2017). Therefore, Hallam and Zanella explained that this behavior creates the privacy paradox with the result of the privacy calculus between risks and rewards. Metzger (2007) had previously not found a strong concern for privacy, and she explained this with the privacy paradox. More recent research has sought to further explain or even dismiss the privacy paradox. For example, Trepte et al. (2020) argued that their findings were against the privacy paradox. They found that users who had higher privacy concerns disclosed less information. As previously noted, their findings supported prior research that suggested social support impacted information disclosure. Researchers continue to argue the cause and the existence of a privacy paradox online; therefore, important questions regarding the privacy paradox remain unanswered. Further exploration is needed of other variables that may present as the privacy paradox, such as digital privacy fatigue.

Digital Privacy on Social Media

Social media has become an important communication channel in today’s digital society. It provides not only a way for friends and family to connect but also a forum for free speech and political discourse. Additionally, social media is heavily used for consuming and sharing news and information, helping users stay up to date on current events (Bergström & Belfrage, 2018). Trepte (2020) argued that freedom and privacy are historically closely related, which is also the case when it comes to social media and other online platforms. Privacy control on social media is limited, which Trepte noted can be frustrating and stressful for users. There will never be complete control of privacy over social media networks; however, social media companies should strive to give users enough control over their data so that users feel safer and more willing to disclose information. Each social media platform is different thus having its own privacy tools and management. Masur (2019) noted that privacy research cannot be focused on one particular platform due to the multimodal communication of users. Consequently, users' communication and disclosure behaviors vary among social media platforms.

Yang et al. (2016) explored the privacy culture of students in the United States and Taiwan, comparing the cultural differences of privacy concerns on social media. The results found that students in both countries were concerned with how their information is being used by businesses and their decision-making process. Taiwanese students were more concerned with how their data is perceived by friends and family members, while U.S. students were more concerned about ethics. The U.S. students felt that their data is their property. Another interesting result is that users who feel they have more control of their data will spend more time on that social media platform. Punj (2019) noted that the need for privacy control was a strong influence on limiting the sharing of personal information on social media. Users were more likely to limit personal information on social media if they had experienced a privacy violation in the past (Punj, 2019). While this study points to control as a strong influence on information disclosure, it does not address whether it is perceived control over privacy or actual effective control measures that influenced users to disclose more information. It could be suggested that simply users' perception of control may be enough to promote information sharing.

When Mosteller and Poddar (2017) examined users' privacy protection behavior in relation to their social media engagement, they found that trust influences social media disclosure. Therefore, when users feel that they have some type of control over their privacy, they are more trustworthy of the website and more willing to share information. If there is a privacy breach, users were less likely to engage with the website (Mosteller & Poddar, 2017). Jozani et al. (2020) determined similar results; privacy concerns reduce social media engagement. However, privacy control was found to only impact social privacy and not institutional privacy (Jozani et al., 2020). As in previous studies, users implement a cost versus benefit analysis when sharing information online (Jozani et al., 2020). Often, even if users are aware of possible privacy violations, they may have a false sense of control through privacy settings (Jozani et al., 2020). Previously, Hunter and Taylor (2020) had also found that users' preference for privacy directly impacts the frequency and duration of social media use. A user's individual experience as well as an experience of acquaintances on social media has shown to be an important catalyst for privacy protection behavior (Alkire et al., 2019).

College Students and Digital Privacy

Many studies have suggested that college students adjust their privacy protection behavior and information disclosure on social media according to the situation (Choon, 2018; Liu et al., 2017; Quinn & Papacharissi, 2018; Xie & Karan, 2019). Liu et al. (2017) explored college students' privacy management and disclosure behavior on Facebook and found this to be true. Additionally, when examining the data by gender, they found that men had privacy settings that were more open and that men disclosed more information than women. However, they found that more privacy control would produce more information disclosure. Students that have more knowledge of social media privacy settings were more likely to frequently adjust those settings depending on the situation and amount of information they wished to disclose (Liu et al., 2017). Digital literacy of college students, therefore, plays an important role in their privacy protection behavior.

When comparing social media platforms, a study by Choon (2018) indicated that most college students feel privacy is important to protect their reputation on Facebook; however, on Twitter, publicity was more important. They also found that students utilize self-censorship to protect their privacy and only occasionally disclose geolocation. Facebook's privacy controls were utilized, such as limiting to friends only. When determining boundaries between online and offline, students found it much more difficult to protect privacy online (Choon, 2018). In other research, Quinn and Papacharissi (2018) found that college students' motives for social media use and their tools for privacy management depended on the situation. They coined the term "liquid privacy" (p. 60) to describe the way users adapt their privacy protection behavior to meet the situation.

In their study, Xie and Karan (2019) discussed similar findings that college students created different privacy boundaries for personal information, such as blocking companies from accessing personal information. They found that students protected privacy by using boundaries to prevent access to their personal information, such as phone number or email address; this was the strongest type of boundary. However, when sharing information about interests, such as the type of music, movies, or books they like, students often had fewer boundaries. These studies suggested that college students weigh the risks of privacy violations versus the benefits of information disclosure online.

Experiencing online turbulence may be one of the factors motivating users to adapt privacy management and information disclosure. Litt and Hargittai (2014) noted that over a third of the young adults they surveyed had experienced some type of turbulence online, ranging from small privacy breaches to more complex issues that impact their school or work. Young adults also were found to perceive more control over their privacy and data when given control over cookie tracking (Bornschein et al., 2020). When looking at the issue from a marketing perspective, companies may increase purchase intention by giving young consumers more control and power over how their data is collected and used (Bornschein et al., 2020). As previous research has noted, control may also increase information sharing on social media sites (Liu et al., 2017; Punj, 2019).

Digital Literacy

Digital privacy and online privacy protection behavior cannot be discussed without addressing their connection to digital literacy. Park (2011) defined digital literacy as an idea that "encompasses critical understanding of data flow and its implicit rules for users to be able to act" (p. 217). Furthermore, Park stated that digital literacy "may serve as a principle to support, encourage, and empower users to undertake informed control of their digital identities" (p. 217). If users do not possess basic knowledge of digital technology and data surveillance, they cannot effectively manage their online privacy. Trepte et al. (2015) suggested that a lack of digital and privacy literacy may explain the privacy paradox. As Trepte (2020) noted, privacy is critical to digital communication, but not all users have the same opportunities due to the lack of digital literacy. Users' lack of knowledge limits their response to privacy turbulence and their privacy management behavior (Trepte et al., 2015).

Digital literacy is a critical skill for college students who are often managing their online identity on their own for the first time after they no longer have parental or school restrictions (Magolis & Briggs, 2016). Students are often lacking in digital literacy and effective privacy protection behavior. Adorjan and Ricciardelli (2018) observed that teens do employ some privacy protection behavior; however, they also struggle with the privacy paradox. This may be explained by teens' lack of digital or privacy literacy. Digital literacy is key because abstaining from social media and digital technology is not an option for college students in today's digital world (Adorjan & Ricciardelli, 2018). Luke and Sefton-Green (2018) argued that digital literacy will give students the tools needed to navigate their digital environment. Additionally, Xie and Karan (2019) found that college students with higher digital literacy were more likely to use privacy protection behavior to safeguard personal information.

Digital Privacy Literacy

Privacy literacy is a specific aspect of digital literacy that addresses users' knowledge of digital privacy management and digital data protection laws (Trepte et al., 2015). Privacy literacy is defined by Trepte et al. (2015) as "a combination of factual or declarative ('knowing that') and procedural ('knowing how') knowledge about online privacy" (p. 339). Digital privacy literacy describes how users protect their personal data and online information. Researchers have suggested that a lack of privacy literacy may play a role in explaining privacy behavior online and the privacy paradox (Park, 2011; Trepte et al., 2015). While some research has shown a correlation between the two, Sindermann et al. (2021) found that they were only moderately related. Therefore, they argued that their research suggested other variables also impact online privacy protection behavior and the privacy paradox. Other factors that contribute to the privacy paradox should be examined.

Masur et al. (2017) found a connection between higher knowledge about data protection and data protection laws and users' privacy protection behavior. However, this particular study was conducted in Germany and examined European privacy protection law. It is unclear if the results could be replicated in a country such as the United States due to the lack of comprehensive data privacy regulations. Similarly, Baruh et al. (2017) surveyed llyparticipants from 34 countries, finding that users with higher privacy literacy had a higher concern for privacy. Moreover, Masur (2019) noted that current research has not determined the type of privacy literacy skills needed to successfully navigate privacy regulations nor is it clear that higher privacy literacy actually encourages privacy management online. Other factors influence privacy management behavior such as personality, gender, and intelligence (Sindermann et al., 2021).

Digital Citizenship and Digital Literacy

Another key aspect of digital literacy is digital citizenship. Mossberger et al. (2008) defined digital citizenship as "the ability to participate in society online" (p. 1). They argued that the Internet influences social culture and facilitates citizens' participation in society. Furthermore, they described people who use the Internet on a daily basis as digital citizens. Hintz et al. (2017) stated that everyone is a digital citizen who uses digital media to engage with society. They posited that digital citizenship is defined by users' actions online. When researching college students, Kara (2018) found that most students defined digital citizenship as simply "a person's identity on the Internet" (p. 183). Gleason and von Gillern (2018) and Hintz et al. (2017) both argued that digital citizenship is more than simply online participation or an online identity.

Digital citizenship is directly related to digital literacy. To be a contributing and effective digital citizen, users must have a high level of digital literacy. Gleason and von Gillern (2018) argued that there is a need for digital literacy instruction in an educational setting so that students learn to become responsible digital citizens. Social media platforms have created a new form of citizenship and have changed how educators think of literacy (Gleason & von Gillern, 2018). Xu et al. (2019) stated that "the modern introduction of social media into society is a massive technological change influencing all demographic segments of humanity in personal, educational, and professional domains" (p. 736). Additionally, Yu et al. (2019) argued in their research that digital citizenship is a subfield of digital literacy because digital citizenship is formed through online engagement that results in civic discussion and participation. This type of civic participation is most often on social media networking sites, and the most active users of social media are college students (Yu et al., 2019). It is, therefore, pertinent to study the digital citizenship behavior and digital literacy of college-aged users of social media platforms.

Researchers have argued that there is a digital divide among users (Madden et al., 2017; Park, 2011). One aspect that may impact the digital divide is a user's cognitive level (Park, 2011). A user's expertise may affect a user's citizenship behavior online as well as their privacy protection behavior (Park, 2011). Dogruel and Jöckel (2019) also argued that a lack of resources contributes to not only the frequency of Internet use but also digital privacy. According to Luke and Sefton-Green (2018), the current dynamic of digital communication and technology "requires a remaking of citizenship, ethics, and a renewed social contract" (p. 6). They stated that digital literacy is key to promoting responsible digital citizenship.

When it comes to digital privacy, Hintz et al. (2017) observed that surveillance and data collection online has a significant impact on and creates a challenge for digital citizenship. They further noted that people are not digital citizens only because of their use of the Internet but also for the data footprints left behind from online activity. Companies gather, store, and sell users' data (Hintz et al., 2017). This is what Lyon (2017) has termed surveillance culture. According to Lyon (2017), surveillance culture is a result of digital modernity. He defined it as a culture because surveillance is now something that everyone must face in the digital world. Lyon argued that "surveillance has become so pervasive that the majority comply without questioning it" (p. 829). This has especially become prevalent in the use of social media. Users must agree to terms and agreements that are full of legal jargon that most citizens cannot understand. Most users feel they have little to no control over how their data is used online (Dogruel & Jöckel, 2019).

Dogruel and Jöckel (2019) also argued that privacy and surveillance are cultural, noting that all cultures have created their own forms of privacy protection and control. They relate this to communication privacy management theory, which states that culture influences privacy rules. Culture aids in defining a person's values, which includes their views on privacy. This can be seen on social media platforms among the sharing behavior of users. Dogruel and Jöckel (2019) proposed that researching the digital communication habits of Generation Z college students will provide further insight into their digital culture.

Privacy Fatigue

While much research has been conducted regarding privacy concern, the privacy paradox, and other privacy behavior, little research has been conducted on the impact of privacy fatigue on users' privacy protection behavior. Privacy fatigue is defined by Choi et al. (2018) as "a sense of weariness toward privacy issues, in which individuals believe that there is no effective means of managing their personal information on the Internet" (p. 42). Choi et al. highlighted the phenomenon of privacy fatigue in their study that explored how privacy fatigue impacted online privacy protection behavior. Their results found that privacy fatigue has a greater impact on privacy protection behavior than privacy concern. They noted that privacy fatigue is “a coping strategy of behavioral disengagement” (p. 43). Researchers have called privacy fatigue by other terms, such as privacy cynicism (Lutz et al., 2020), privacy apathy (Hargittai & Marwick, 2016), and surveillance realism (Dencik & Cable, 2017). Researchers have suggested that privacy fatigue may be an important variable that explains the privacy paradox (Choi et al., 2018; Lutz et al., 2020).

Tang et al. (2020) explored privacy fatigue in online disclosure by suggesting the concept of privacy fatigue as a theory. They noted that privacy fatigue includes the influences of privacy risk and privacy breaches. Citing Boksem et al. (2005) and Dhir et al. (2019), Tang et al. noted that privacy fatigue may reduce users’ participation and attention, causing withdrawal from communication online. Additionally, citing Keith et al. (2014), they noted the importance of privacy control and how it impacts users’ intention to disclose information. Users who feel higher levels of privacy fatigue will experience more cynicism, exhaustion, and frustration. Their results found that both privacy fatigue and privacy concern influenced users’ intention to disclose information online; however, privacy fatigue was the strongest influence.

Social Network Fatigue

Privacy fatigue is closely related to social network fatigue. Ravindran et al. (2014) defined social network fatigue as “a subjective, multidimensional user experience comprising feelings such as tiredness, annoyance, anger, disappointment, guardedness, loss of interest, or reduced need/motivation associated with various aspects of social network use and interactions” p. 2317). Research suggests that users’ privacy concern on social media can create social network fatigue (Zhu & Bao, 2018). Greater privacy concern promotes greater social media fatigue (Logan et al., 2018). When social media platforms give users more control over their privacy management, privacy concerns can be reduced thus reducing social network fatigue (Logan et al., 2018; Zhu & Bao, 2018). Logan et al. (2018) noted that the more users access and rely upon social media platforms the greater their privacy concern. It is key for social media companies to make sure their settings are easy for users to access and understand (Logan et al., 2018). They suggested that “Fear of Missing Out” (FOMO) on social media may encourage social media communication despite privacy concerns, but this should be further explored in future research.

Current Research Gaps

Because privacy fatigue is a relatively new term used to describe digital privacy behavior, Choi et al. (2018) recommended further research into how privacy fatigue impacts online protection behavior. Tang et al. (2020) built upon the research of Choi et al. by studying not only privacy fatigue and privacy concerns but also how personality traits impact those factors. Tang et al. examined the role of privacy fatigue in the disclosure behavior within mobile applications. They found that privacy fatigue has a greater impact on behavior intention than privacy concern. Additionally, they noted that there is little research into privacy fatigue and its relation to privacy concern. Furthermore, it is noted that personality traits, such as neuroticism and agreeableness, play a key role in the level of privacy fatigue. Their research introduced an emotional component to digital information disclosure behavior that had not been previously explored. Finally, further research is suggested on how privacy fatigue impacts users’ other decisions and what additional factors impact privacy fatigue in other online settings.

Like Tang et al. (2020), De Wolf (2020) sought to expand upon the privacy fatigue research of Choi et al. (2018). De Wolf studied teens and their privacy management on social media. Tang et al. and De Wolf suggested that privacy fatigue could explain the privacy paradox. De Wolf argued that attempting to manage personal privacy on social media feels futile because the openness of social media makes digital privacy challenging. He also argued that people may even acquire a false sense of security from protection measures that are not effective. De Wolf utilized CPM theory framework to examine privacy protection behavior and privacy fatigue. He posited that the narrow definition of privacy management given by CPM theory would suggest that "sharing any personal information on social media could be equated with giving up one's privacy" (p. 1061). Therefore, CPM theory is too limiting for defining digital privacy protection. He recommended further research into privacy fatigue or defeatism in relation to privacy turbulence and highlighted CPM theory's failure to address privacy fatigue as it relates to online privacy management. Therefore, this study seeks to expand upon privacy fatigue research within the framework of CPM theory.

Generation Z

Compared to the Millennial generation, Generation Z, or Gen Z, has been researched and studied very little, yet Gen Z is quickly growing up and influencing current social trends. Gen Z has been labeled iGen with the "i" representing the Internet and its strong influence over their lives (Twenge, 2017). Current college students of Gen Z are the first generation to have grown up in a digital environment; therefore, they are a digitally literate generation that views social media as an integral part of everyday communication (Marron, 2015; Rospigliosi, 2019; Turner, 2015). Researchers argue that Gen Z is different than any other generation before it because of how digital communication and technology have permeated their lives (Parker & Igielnik, 2020; Twenge, 2017). Growing up in a digital environment, Gen Z's social culture goes against previous social norms in how they communicate as well as in their attitudes toward social issues

(Parker & Igielnik, 2020; Twenge, 2017). Twenge (2017) argued that this change in social culture is driven by smartphones. Gen Z is the first generation to begin their teen years with access to smartphones, and the first generation to have access to social media networks their entire lives (Twenge, 2017).

Demographics of Generation Z

Generation Z represents those born after 1996 with the oldest of the generation now in college or recently graduated (Marron, 2015). This generation makes up approximately 24% of the U.S. population with 74 million people (Twenge, 2017). According to Marron (2015), “Gen Z students will have had the highest rates of homeschooling in the U.S. history and will be accustomed to order, structure, a strong work ethic, and a sense of predictability” (p. 123). Compared to other generations, American Gen Z citizens are the most racially and ethnically diverse and are predicted to be the most educated generation to date (Parker & Igielnik, 2020). Additionally, Gen Z is less religious, more independent politically, and more inclusive, seeking equality and freedom of expression (Twenge, 2017).

When marketing to Generation Z, it is important to note that authenticity is important to this generation (Mathew, 2020; Puiu, 2016). Additionally, this generation responds to edgy campaigns and are strong consumers and producers of content (Mathew, 2020). Furthermore, Gen Z prefers mobile devices over laptops and other larger devices, and their values have a major impact on their buying habits (Fontein, 2019; IBM, 2017). According to a 2021 Pew Research Center poll, YouTube is the most popular social media platform. In the 18-29 age bracket, 95% use YouTube (Pew Research Center, 2021). That is the highest usage of the site of any demographic. Facebook and Instagram were the other social media platforms more frequently used by the younger age group (Pew Research Center, 2021). For online shopping, Gen Z prefers social media apps or specialized store apps such as Amazon (Priporas et al., 2017). Additionally, Gen Z likes the advantages of digital payment options like Apple Pay or PayPal due to convenience (Priporas et al., 2017). It is no surprise that the digital generation prefers all things digital. Digital technology provides one aspect that Gen Z highly desires—convenience (Wood, 2013).

Social Media and Communication Practices of Generation Z

Many researchers noted that Gen Z prefers digital communication over more traditional methods—even preferring a quick text to an email (Beck & Wright, 2019; Marron, 2015; Seemiller & Grace, 2019). However, Seemiller and Grace (2019) discovered that 83% of Gen Z respondents preferred face-to-face communication over other communication methods—even above texting. This may explain why video chat platforms are so popular with this generation. While Gen Z respondents reported preferring face-to-face communication, 60% also reported their preference for texting, which includes messaging apps such as WhatsApp and Facebook Messenger (Seemiller & Grace, 2019). Like Beck and Wright (2019), Seemiller and Grace also found that Gen Z is not a fan of traditional phone calls or email. Instead of using their smartphones for a phone call, Gen Z utilizes their devices to access video chat and social media platforms (Seemiller & Grace, 2019).

Social media is not only seen as a communication tool for Gen Z but also as an educational tool (Rospigliosi, 2019). With technology such an integral part of Gen Z's life, it is critical to study the privacy protection behavior that they employ on social media platforms. Beck and Wright (2019) noted that the social norms of Gen Z have changed the boundaries of what is public and what is private. Although this generation has been described as risk avoiders, some researchers suggested that the same behavior does not appear to be carrying over to sharing information on digital media (Adorjan & Ricciardelli, 2019; Beck & Wright, 2019). However, Yerby et al. (2019) found that most of the college students surveyed feel it is risky to share personal information on social media. They also found students believe there are often privacy breaches that are out of the user's control. In contrast, another study found that Gen Z students felt they had nothing to hide, so privacy was not viewed as important (Adorjan & Ricciardelli, 2019).

Building on prior research that connects trust and privacy protection behavior, Koohang et al. (2018) found that college students with higher privacy concerns were less likely to trust social media platforms with personal information and felt that social media is risky. While the Koohang et al. study surveyed a large number of students and staff, Magolis and Briggs (2016) conducted a smaller study with eight undergraduates. They found that some of the students were unwilling to share locating information, while other students felt the networking opportunities were worth the risk to privacy (Magolis & Briggs, 2016). Some of the students even felt that the fear of online identity theft was not realistic (Magolis & Briggs, 2016). Similarly, Choi and Sung (2018) noted that this younger generation felt the benefits of digital technology, particularly within their social life, were greater than the risk of privacy breaches. Digital communication is such an integrated part of Gen Z's life that they seem to be willing to take on some privacy risk. However, researchers have also found that Gen Z will adapt their privacy protection behavior depending on the situation, such as the particular social media platform or intended audience (Quinn & Papacharissi, 2018).

Summary

The current literature on digital privacy and CPM theory suggests that other variables may play a part in creating the privacy paradox. While there is wide agreement that a privacy paradox exists, views differ on what exactly causes the discrepancy between privacy concerns and information disclosure online. Earlier studies suggested that the privacy paradox was created by a lack of control (Baruh et al., 2017; Punj, 2019); however, more recent research has suggested that other factors, such as privacy fatigue, contribute to users' discrepancy between their privacy concerns and their privacy behavior (Choi et al., 2018; Tang et al., 2020). More specifically, it appears that no studies have investigated the impact privacy fatigue has on the privacy concerns of Generation Z college students. This digital generation approaches technology and social media differently than any other generation before. They are digitally savvy, yet they must still navigate the difficult task of online privacy management. Therefore, this study sought to explore how privacy fatigue impacts the privacy protection behavior of Generation Z college students.

CHAPTER THREE: METHODS

Overview

The purpose of this study was to employ communication privacy management (CPM) theory to examine the privacy management behavior of Generation Z college students, specifically within the variables of privacy fatigue, privacy concern, privacy control, and privacy management. This chapter focuses on the methodology used to answer the research question and hypotheses. Based on previous CPM theory and privacy fatigue research, a quantitative approach was employed via an online survey. The research design, participants, procedures, and data analysis are presented in this chapter.

Method and Design

A quantitative research method with a correlational research design was used for the study of Generation Z college students and their privacy protection behavior. The study was conducted with a postpositivist research philosophy, which Creswell and Creswell (2018) noted is a more traditional research design. A postpositivist approach reflects “the need to identify and assess the causes that influence outcomes” (Creswell & Creswell, 2018, p. 6). It utilizes the scientific method to verify theory and allows researchers to observe independently (Creswell & Creswell, 2018). This study took a deductive research approach utilizing CPM theory.

Data was collected via an online, cross-sectional survey through Amazon Mechanical Turk. The focus population was Generation Z college students—specifically those born between 1995 and 2003—who prefer to communicate through digital technology (Marron, 2015). Using an online survey is a quicker and easier method to retrieve information. Additionally, online surveys allow for access across multiple devices, including smartphones (Vehovar & Manfreda, 2017). The use of an online survey was important for the target population, as past research found that 75% of Generation Z preferred a smartphone as their most frequently used device (Fontein, 2019; IBM, 2017). College students cannot be relied upon to mail in a survey or to take the time to answer survey questions in person or over the phone (Marron, 2015). Generation Z especially prefers to communicate digitally (Beck & Wright, 2019; Marron, 2015; Seemiller & Grace, 2019). Additionally, utilizing an online survey is a cost-effective method for collecting data from a large sample of the target population (Vehovar & Manfreda, 2017).

A quantitative methodology with a 7-point Likert-type survey was implemented for this study because it was modeled after previous research studies within the framework of CPM theory (De Wolf, 2020; Kennedy-Lightsey et al., 2012; Metzger, 2007; Xie & Karan, 2019; Xu et al., 2011; Yang et al., 2016). For example, Yang et al. (2016) conducted a quantitative research study examining the privacy protection behavior of college students on Twitter. Both Yang et al. (2016) and Xie and Karan (2019) utilized an online 5-point Likert-type survey method with a convenience sample from universities. Xu et al. (2011) conducted a quantitative survey with an online 7-point Likert-type survey assessing users' digital privacy concern. A quantitative study by De Wolf (2020) utilized a 7-point Likert-type survey to assess Belgian teens' digital privacy management. He employed CPM theory and noted the need for further research into privacy fatigue as it relates to online privacy management. These studies provide the foundation for the proposed research.

Operational Definitions of the Variables

For clarity, the four variables in the study have been defined below:

- **privacy fatigue**: the weariness, frustration, burn-out, and/or lack of effectiveness felt when trying to manage personal privacy on social media

- **privacy concern**: the concern or worry that one's private information could be made public or that embarrassing information could be shared when using social media
- **privacy control**: the feeling of whether or not one is in control of personal information that is shared online
- **privacy management**: the actions taken to protect privacy within social media networking sites, such as limiting posts to friends or untagging oneself in a photo

Research Question and Hypotheses

The following research question and hypotheses were created to explore the online privacy management behavior of Generation Z college students. Previous research has focused heavily on the impact privacy concern has on information disclosure and digital privacy management (Barnes, 2006; Gerber et al., 2018; Masur & Trepte, 2020; Xie & Karan, 2019). As of this writing, there is limited research investigating the impact of privacy fatigue (Choi et al., 2018; De Wolf, 2020). Therefore, this study sought to build upon past digital privacy studies and incorporate the influence of privacy fatigue. Additionally, this study sought to expand CPM theory research by examining the relationship between privacy fatigue and privacy management.

RQ 1: Does communication privacy management theory explain the relationship between privacy fatigue and privacy concern in Generation Z college students?

H1: Generation Z college students that exhibit a higher level of privacy concern will feel a higher level of privacy fatigue.

H2: Generation Z college students that exhibit a higher level of privacy concern feel less control over their online privacy.

H3: Generation Z college students who express a higher level of privacy concern will utilize more privacy management strategies on social media.

H4: Generation Z college students with a higher level of privacy fatigue will feel they have less control over their online privacy.

H5: Generation Z college students with a higher level of privacy fatigue will employ less online privacy management strategies.

H6: Generation Z college students who utilize more privacy management strategies will feel more control over their privacy on social media.

H7: Female Generation Z college students exhibit more privacy concern and privacy fatigue than male Generation Z college students.

Participants and Setting

A convenience sampling method was used to survey 1000 Generation Z college students. After data cleaning, 892 valid responses were left, which exceeded the adequate sample size. The survey was published on Amazon Mechanical Turk and open to residents of the United States. Screening questions were used to exclude participants who were not between the ages of 18-25 (born between the years 1996 and 2003) and had not taken any college courses.

Generation Z currently makes up 20% of the population with approximately 67 million people in the United States (Statista, 2021). The sample number was determined based on the U.S. Generation Z population via a sample size calculator, which resulted in a suggested sample size of 385 participants. In addition, a power analysis was conducted using free downloadable software, G*Power 3.1. According to the power analysis, the minimum sample size needed for a Pearson *r* with a medium effect size, a minimum power of 0.80, and an alpha of 0.05 was 84.

The final sample included 59% male and 41% female respondents (see Figure 1). Respondents were asked about their preferred device for accessing social media with 58% preferring a smartphone, 25% preferring a laptop, 13% preferring a desktop, and 3% preferring a tablet (See Figure 2). When asked their preferred platform, 69% preferred Android, while 29% preferred iOS (see Figure 2).

Figure 1

Male and Female Respondents

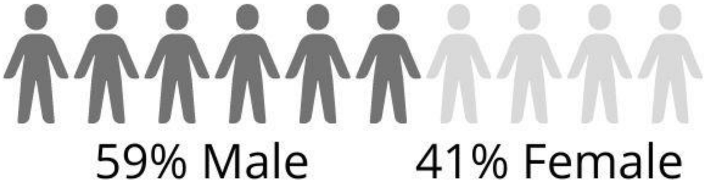
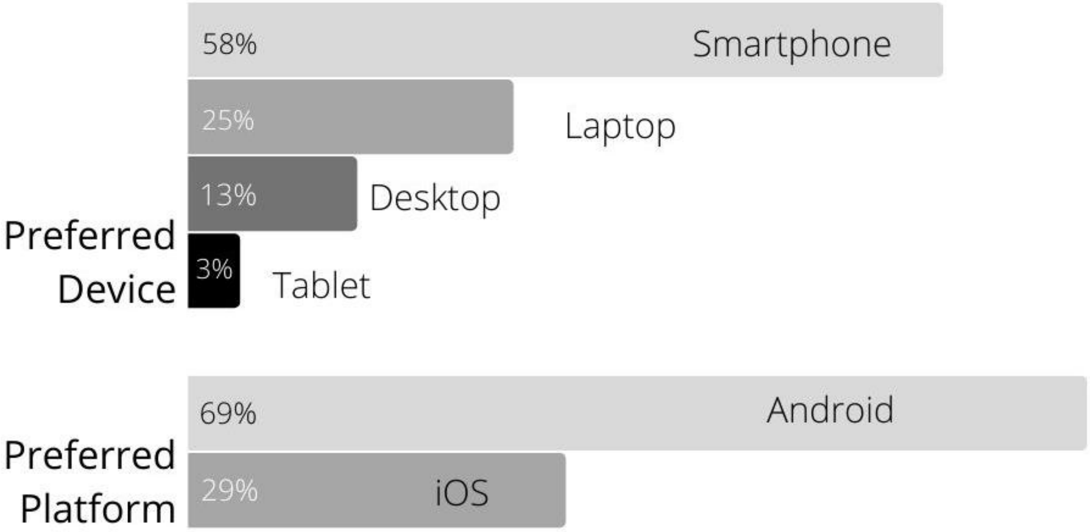


Figure 2

Preferred Device and Platform



Participants were asked their race or ethnicity with 77% responding as White, 9% as Black, 7% as Hispanic, and 5% Asian or Pacific Islander. Regarding education, 60% stated they have completed a bachelor’s degree and 18% are currently enrolled or have taken some college courses. When asked about political views, 54% responded with conservative-leaning views, while 34% responded with liberal-leaning views. Finally, 49% stated they were Christian, and 34% stated they were Catholic. See Table 1 for the complete list of sociodemographic characteristics of the participants.

Table 1

Sociodemographic Characteristics of Participants

		Frequency	Percent
Race/Ethnicity	White	683	76.6%
	Black/African American	84	9.4%
	Hispanic	58	6.5%
	Asian/Pacific Islander	42	4.7%
	Native American or Alaskan Native	13	1.5%
	Other	10	1.1%
Education	High School Degree or Equivalent	43	4.8%
	Trade School	2	0.2%
	Currently enrolled or have taken courses	156	17.5%
	Associate Degree	64	7.2%
	Bachelor’s Degree	532	59.6%
	Master’s Degree	95	10.7%
Political Views	Slightly Conservative	212	23.8%
	Very Conservative	270	30.3%
	Neutral/Neither Conservative or Liberal	94	10.5%
	Slightly Liberal	139	15.6%
	Very Liberal	165	18.5%
	Prefer not to say	8	0.9%
Religion	Christian	437	49.0%
	Catholic	305	34.2%
	Agnostic	42	4.7%
	Atheist	37	4.1%
	Prefer not to say	18	2.0%
	Muslim	14	1.6%
	Hindu	14	1.6%
	Jewish	11	1.2%
	Other	8	0.9%

Instrumentation

The data was collected via a web-based, cross-sectional survey with 7-point Likert-type questions, ranging from “strongly agree” to “strongly disagree” (see Appendix). The survey questions were adapted from the research instruments developed by Choi et al. (2018) and De Wolf (2020). The privacy fatigue scale was adapted from Choi et al. (2018) and included five Likert-type questions that assessed respondents’ burn-out from managing digital privacy. The privacy management scale was adapted from De Wolf (2020) and included five Likert-type questions which assessed respondents’ social media privacy settings. The privacy concern scale was adapted from De Wolf (2020) and contained four Likert-type questions which assessed respondents on their level of concern for their digital privacy. The privacy control scale was adapted from De Wolf (2020) and contained five Likert-type questions which assessed respondents on how much control they feel they have over their digital privacy. The scales and their reliability are discussed in depth in Chapter 5. Finally, the questions were reviewed by faculty for any potential issues.

A 7-point scale was chosen not only because the research is modeled after previous privacy studies (Choi et al., 2018; De Wolf, 2020; Tang et al., 2020) but also because previous research has suggested that a 7-point scale more accurately measures participant responses than a 5-point scale (Finstad, 2010). A 7-point Likert-type scale was also found to be more appropriate for unsupervised, electronically-distributed questionnaires (Finstad, 2010). The survey included 19 Likert-type questions that contained the underlying constructs of privacy concern, privacy fatigue, privacy control, and privacy management. Other data collected included gender, race or ethnicity, age, education, political view, religion, preferred technological device, and technology platform use.

Procedures

First, institutional review board approval was acquired. IRB application and approval is an important part of the process in human research as it seeks to ensure human research participants are protected from harm (Pritchard, 2011). Under the Office of Human Research Protection, the IRB also protects the researcher and institution by ensuring ethical research methods (Pritchard, 2011). The IRB weighs the risks of participants with the potential benefits of the research. The IRB application for this study included the research question and hypotheses, target population, recruitment method, data security plan, informed consent, and the survey questions.

After IRB approval, the survey was created using Qualtrics, which is a mobile-friendly software program used to create and host the survey and the collected data. Next, the Qualtrics survey link was published on Amazon Mechanical Turk, which is a crowdsourcing marketplace used to recruit participants. Data collected from Amazon Mechanical Turk has shown to be reliable because those requesting data have the ability to reject work, which motivates workers to follow instructions and complete requests with attention (Sheehan, 2018). The publication of the survey was limited within Amazon Mechanical Turk to those based in the United States. Pre-qualifying questions regarding education and age were utilized within the survey to screen participants. The survey was published on December 22, 2021 and was open until 1,000 surveys were collected, which was approximately four days. A total of 892 valid responses were used for data analysis.

Data Analysis

The survey data was downloaded from Qualtrics and imported into Excel for cleaning. First, all respondents not between the ages of 18-25 (born between the years 1996 and 2003) were removed as well as any blank responses for age and education since it could not be determined if the respondents met the required criteria. Further, any responses that had a blank answer for any of the 19 core privacy-related questions were removed. Three extreme outliers within time duration were removed—281,372; 26,413; and 24,145 seconds. A Z score was then used to determine other outliers in time duration. Any answers with a Z score of + 3.0 were removed. Responses that took 60 seconds or less to complete the survey were removed. There is no clear method for the elimination of time outliers; therefore, researchers must develop the method best fit for their study (Matjasic et al., 2018). A more conservative approach was taken to eliminate shorter and longer time responses to not delete valid responses. This resulted in keeping response times between 1 and 20 minutes. Finally, 15 responses were removed for straight-line answers or nondifferentiation—when respondents choose the same response for all items—which has been shown to compromise data (Yan, 2008). The final valid number of respondents was 892.

The data was then imported into SPSS for analysis. Descriptive statistics including the mean, standard deviation, and number were calculated for the four scales. Cronbach's alpha was used to determine reliability of the scales for each of the four underlying constructs. For data analysis, a series of parametric tests were chosen because each variable was formed by creating a composite score from the mean. This allowed the data to be tested as continuous. Parametric tests have been found to be more robust and to give better results than non-parametric tests (Norman, 2010). To begin data analysis, a Pearson's *r* was first performed to determine the correlation between the variables of privacy fatigue, privacy concern, privacy control, and privacy management. The Pearson's correlation assumes the variables are linearly related (Wrench et al., 2019). The linearity assumption was assessed graphically using a scatterplot. A

Pearson's *r* correlation is the appropriate bivariate statistic when both input variables are continuous and are linearly related.

Next, a multiple linear regression was conducted to determine if the variables privacy concern, privacy control, and privacy management predict privacy fatigue. A multiple linear regression is the appropriate test to use when including two or more predictor variables (Denis, 2020). Variables were evaluated by what they add to the prediction of the dependent variable which is different from the predictability afforded by the other predictors in the model. The F-test was used to assess whether the set of independent variables collectively predicts the dependent variable. R-squared, the multiple correlation coefficient of determination, was reported and used to determine how much variance in the dependent variable can be accounted for by the set of independent variables. The t-test was used to determine the significance of each predictor, and beta coefficients were used to determine the magnitude of prediction for each independent variable. For significant predictors, every one unit increase in the predictor, the dependent variable will increase or decrease by the magnitude of the unstandardized beta coefficient.

Finally, independent samples *t*-tests were performed to address H5. The *t*-tests explored the differences in both privacy fatigue and privacy concern between females and males. An independent samples *t*-test is the appropriate statistical test when the purpose of research is to assess if differences exist in the mean of a continuous dependent variable between the levels of a dichotomous independent variable (Denis, 2020). The hypotheses were tested using an alpha value of .05.

Summary

To explore the correlation of the variables of privacy fatigue, privacy concern, privacy control, and privacy management in order to better understand the digital privacy protection behavior of Generation Z college students, a 7-point Likert-type survey was administered to respondents between the ages of 18-25 (born between years 1996-2003). The survey link was posted on Amazon Mechanical Turk, while the survey and data were hosted by the software platform Qualtrics. The data was subsequently cleaned in Excel and imported to SPSS for analysis. Statistical tests included a Pearson's *r*, a multiple linear regression, and independent samples *t*-tests. The results of the data analysis are presented in the following chapter.

CHAPTER FOUR: RESULTS

Overview

The purpose of this study was to explore how privacy fatigue, privacy concern, privacy control, and privacy management impact the communication of Generation Z college students on social media within the theoretical construct of communication privacy management (CPM) theory. The following chapter presents the results and analyses of the data. Data was collected via an online survey that assessed how Generation Z college students feel about their digital privacy. This chapter will begin with the reliability of the scales followed by descriptive statistics. The statistical tests and their results will be described and presented. Finally, the chapter concludes with a summary of the results.

Research Question and Hypotheses

RQ 1: Does communication privacy management theory explain the relationship between privacy fatigue and privacy concern in Generation Z college students?

H1: Generation Z college students that exhibit a higher level of privacy concern will feel a higher level of privacy fatigue.

H2: Generation Z college students that exhibit a higher level of privacy concern feel less control over their online privacy.

H3: Generation Z college students who express a higher level of privacy concern will utilize more privacy management strategies on social media.

H4: Generation Z college students with a higher level of privacy fatigue will feel they have less control over their online privacy.

H5: Generation Z college students with a higher level of privacy fatigue will employ less online privacy management strategies.

H6: Generation Z college students who utilize more privacy management strategies will feel more control over their privacy on social media.

H7: Female Generation Z college students exhibit more privacy concern and privacy fatigue than male Generation Z college students.

Reliability and Descriptive Statistics

The survey contained 19 questions in a 7-point, Likert-type format that addressed digital privacy issues. Of those questions, four were designed to test privacy concern. Five questions per construct were designed to test privacy fatigue, privacy control, and privacy management. The scales were coded so that 1 = strongly disagree and 7 = strongly agree so that a higher number means higher agreement with the statements.

Reliability of the Scales

There is much debate between scholars on the best way to measure and analyze Likert-type data. Often researchers have argued that Likert-type data is ordinal data that must be measured and tested with non-parametric tests. However, more recently, research has suggested that Likert-type data be measured as interval data if it is scaled (Boone & Boone, 2012; Subedi, 2016). Likert-type questions can be measured as interval data when a minimum of four or more Likert-type questions are combined into one variable or scale for the purpose of data analysis (Boone & Boone, 2012; Subedi, 2016). This will result in a quantitative measure of the variables with the mean.

The survey consisted of four underlying constructs which created the variables for the study: privacy fatigue (mean = 5.00, SD = 1.13), privacy concern (mean = 5.24, SD = 0.88), privacy control (mean = 5.19, SD = 1.08), and privacy management (mean = 5.58, SD = 0.88) (See Table 2). Subedi (2016) recommended calculating reliability of the Likert-scale data with

Cronbach’s alpha. Therefore, to test the internal consistency within the underlying constructs, a Cronbach’s alpha was performed. The following sections provide the results of internal consistency as well as the descriptive statistics of the questions within each underlying construct.

Table 2

Descriptive Statistics of the Study Variables

	Mean	Std. Deviation	N
Fatigue	4.9984	1.13302	892
Concern	5.2436	.88344	892
Control	5.1928	1.07920	892
Management	5.5756	.88478	892

Privacy Fatigue: Reliability and Descriptive Statistics

A Cronbach’s alpha score of >0.70 is generally considered acceptable (Pallant, 2010), and at times a score below 0.70 can be acceptable, especially in a scale with a small number of questions (Boyle & Schmierbach, 2020). When the scales contain less items, it can be common to find a lower Cronbach value (Boyle & Schmierbach, 2020; Pallant, 2010). In this case, Briggs and Cheek (1986) recommended also assessing the inter-item correlations for an optimal range of 0.2-0.4.

Five questions were used to measure the construct of privacy fatigue within the survey. The results determined an acceptable internal consistency of α 0.79 (See Table 3). The descriptive statistics for the five questions are included in Table 4. The respondents’ answers indicate they range from neutral to slightly agree within the construct of privacy fatigue.

Table 3

Reliability Statistics: Fatigue Variable

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.791	.793	5

Table 4

Descriptive Statistics for Fatigue Construct

	Mean	Std. Deviation	N
I feel emotionally drained from dealing with privacy issues in an online environment.	5.10	1.472	892
I am tired of online privacy issues.	5.11	1.433	892
It is tiresome for me to care about online privacy.	5.15	1.442	892
I have become less interested in online privacy issues.	4.78	1.657	892
I have become less enthusiastic in protecting personal information provided to social media platforms.	4.86	1.655	892

Note. Adapted from Choi et al. (2018) & De Wolf (2020)

Privacy Concern: Reliability and Descriptive Statistics

Four questions were used to measure the construct of privacy concern within the survey. The results determined an internal consistency of α 0.69 (See Table 5). Because this is borderline acceptable, a review of the inter-item correlations was required, and an optimal range of 0.27-0.42 was found (See Table 6). The descriptive statistics for the four questions are included in Table 7. The respondents' answers indicate they range from neutral to slightly agree within the construct of privacy concern.

Table 5

Reliability Statistics: Concern Variable

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.685	.691	4

Table 6

Inter-Item Correlations: Concern Variable

	Mean	Minimum	Maximum
Inter-Item Correlations	.358	.267	.421

Table 7

Descriptive Statistics for Concern Construct

	Mean	Std. Deviation	N
I am concerned that information I submit to online social media platforms can be misused.	5.38	1.099	892
I am concerned that a person can find private information about me on the Internet.	4.76	1.126	892
I am concerned that others will post embarrassing information about me on social media	5.36	1.448	892
I am concerned about providing personal information to social media platforms because it could be used in a way I did not foresee.	5.48	1.227	892

Note. Adapted from Choi et al. (2018) & De Wolf (2020)

Privacy Control: Reliability and Descriptive Statistics

Five questions were used to measure the construct of privacy control within the survey. The results determined an acceptable internal consistency of α 0.81 (See Table 8). The descriptive statistics for the five questions are included in Table 9. The respondents' answers indicate they lean toward slightly agree within the construct of privacy control.

Table 8

Reliability Statistics: Control Variable

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.810	.810	5

Table 9

Descriptive Statistics for Control Construct

	Mean	Std. Deviation	N
I have little control over online privacy.	5.22	1.459	892
Adjusting my personal privacy settings has little impact.	5.10	1.470	892
It is impossible, as an individual to control my personal information by myself.	5.07	1.465	892
In general, I have the feeling that I can exert little control over my personal information.	5.29	1.412	892
In general, I have the feeling that I can exert little control over my personal information.	5.29	1.353	892

Note. Adapted from De Wolf (2020)

Privacy Management: Reliability and Descriptive Statistics

Five questions were used to measure the construct of privacy management within the survey. The results determined an acceptable internal consistency of α 0.70 (See Table 10). The descriptive statistics for the five questions are included in Table11. The respondents' answers indicate they lean toward slightly agree within the construct of privacy control.

Table 10

Reliability Statistics: Management Variable

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.695	.702	5

Table 11

Descriptive Statistics for Management Construct

	Mean	Std. Deviation	N
I adjusted my settings so that others must ask permission when tagging me in a picture.	5.33	1.497	892
I am careful when accepting friend requests.	5.82	1.206	892
In general, I make use of privacy settings to manage my privacy.	5.76	1.102	892
I untag myself from photos I do not find appropriate.	5.37	1.403	892
I make sure only friends can see my profile on social media.	5.61	1.354	892

Note. Adapted from De Wolf (2020)

Results

To address the research question and the first six hypotheses, two statistical tests were performed. First, Pearson's *r* was performed to determine the correlation between the variables of privacy fatigue, privacy concern, privacy control, and privacy management. Next, a multiple linear regression was conducted to determine if the variables privacy concern, privacy control, and privacy management predict privacy fatigue. The assumptions and results are presented below. Each hypothesis is addressed within the results.

RQ: Does communication privacy management theory explain the relationship between privacy fatigue and privacy concern in Generation Z college students?

H1: Generation Z college students that exhibit a higher level of concern fatigue will feel a higher level of privacy fatigue.

H2: Generation Z college students that exhibit a higher level of privacy concern feel less control over their online privacy.

H3: Generation Z college students who express a higher level of privacy concern will utilize more privacy management strategies on social media.

H4: Generation Z college students with a higher level of privacy fatigue will feel they have less control over their online privacy.

H5: Generation Z college students with a higher level of privacy fatigue will employ less online privacy management strategies.

H6: Generation Z college students who utilize more privacy management strategies will feel more control over their privacy on social media.

Pearson's *r* Correlation

To examine the relationships between the variables of privacy fatigue, privacy concern, privacy control, and privacy management a Pearson *r* correlation was performed using an alpha level of .05 to determine significance. According to Wrench et al. (2019), correlations less than .3 are considered low or weak. Correlations between .3 and .59 are considered moderate, and correlations .6 or higher are considered strong or large.

Assumptions

A Pearson correlation requires that the relationship between each pair of variables is linear (Wrench et al., 2019). This assumption is violated if there is curvature among the points on the scatterplot between any pair of variables. Figure 3, Figure 4, and Figure 5 present the scatterplots of the correlations. A regression line has been added to assist the interpretation. A visual inspection of the scatterplots for each variable shows them to be linear in nature.

Figure 3

Scatterplots with the regression line added for Concern and Management (left), Concern and Fatigue (right)

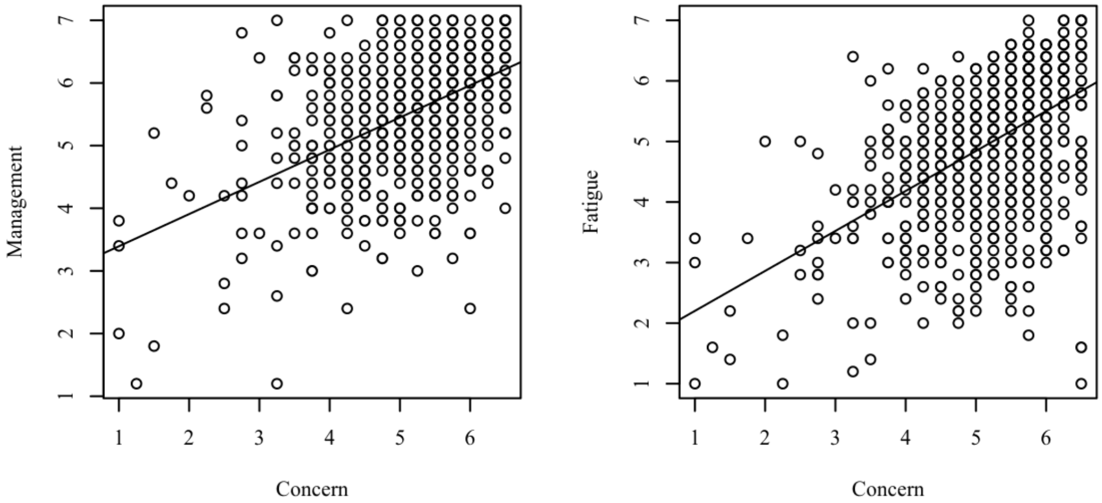


Figure 4

Scatterplots with the regression line added for Concern and Control (left), Management and Fatigue (right)

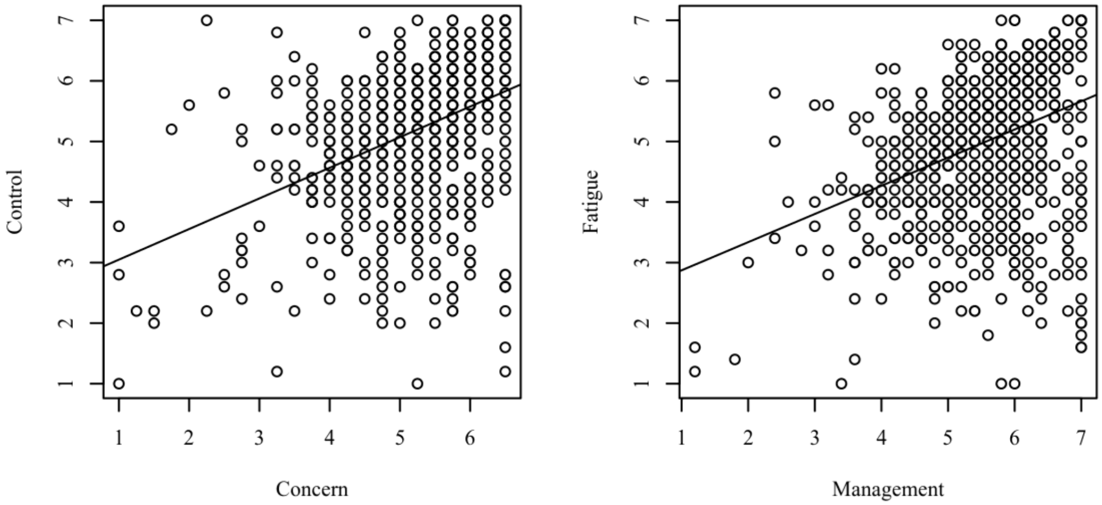
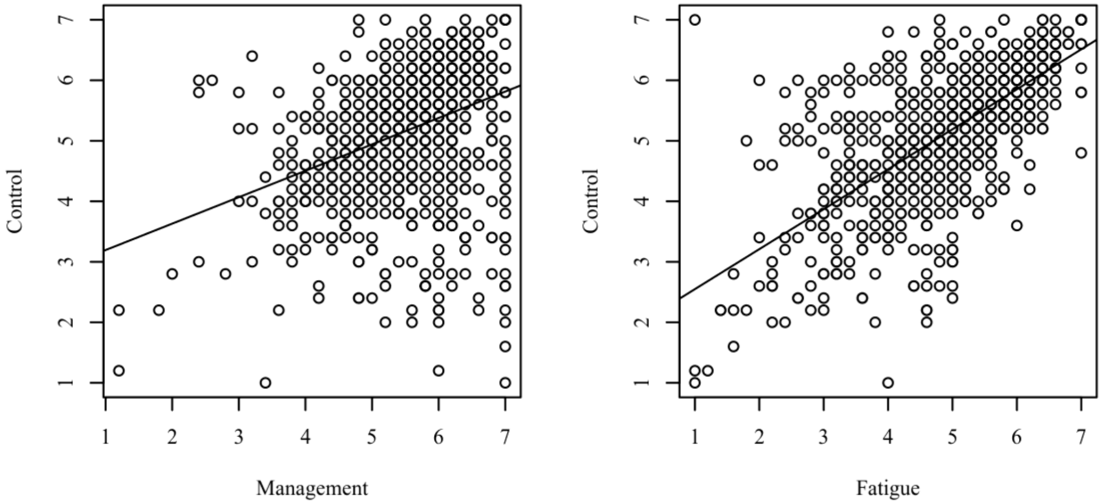


Figure 5

Scatterplots with the regression line added for Management and Control (left), Fatigue and Control (right)



Results of Correlation

Table 12 presents the results of the correlation of the four variables: privacy fatigue, privacy concern, privacy control, and privacy management.

H1. A significant positive correlation was observed between concern and fatigue, with a correlation of .50, indicating a moderate effect size (*p* < .001, 95.00% CI = [.45, .55]). This suggests that as concern increases, fatigue tends to increase. H1 suggested a relationship between privacy concern and privacy fatigue, and it has been supported by a moderate positive correlation.

H2. A significant positive correlation was observed between concern and control, with a correlation of .39, indicating a moderate effect size (*p* < .001, 95.00% CI = [.34, .45]). This suggests that as concern increases, control tends to increase—which, in this case, a higher level of control indicates students increasingly feel less control over their digital privacy. H2 suggested a relationship between privacy concern and privacy control, and it has been supported by a moderate positive correlation.

H3. A significant positive correlation was observed between concern and management, with a correlation of .50, indicating a moderate effect size (*p* < .001, 95.00% CI = [.45, .55]). This suggests that as concern increases, management tends to increase. H3 suggested a relationship between privacy concern and privacy management, and it is supported by a moderate positive correlation.

H4. A significant positive correlation was observed between fatigue and control, with a correlation of .68, indicating a large effect size (*p* < .001, 95.00% CI = [.65, .72]). This suggests that as fatigue increases, control tends to increase, meaning the more privacy fatigue students feel the less control they feel over their privacy. H4 suggested a relationship between privacy fatigue and privacy control, and it is supported by a strong positive correlation.

H5. A significant positive correlation was observed between fatigue and management, with a correlation of .34, indicating a moderate effect size (*p* < .001, 95.00% CI = [.29, .40]). This suggests that as fatigue increases, management tends to increase. H5 suggested that as privacy fatigue increases, privacy management would decrease. Therefore, H5 was not supported.

H6. A significant positive correlation was observed between control and management, with a correlation of .34, indicating a moderate effect size (*p* < .001, 95.00% CI = [.28, .39]). This suggests that as control increases, management tends to increase. H6 suggested a relationship between privacy control and privacy management. A moderate positive correlation is found between the two variables; however, H6 is not supported because an increase in the privacy control variable indicates students feel they have little control over their digital privacy. Managing privacy settings does not appear to make students feel more control.

Table 12

Correlations

		Fatigue	Concern	Control	Management
Pearson Correlation	Fatigue	1.000	.502	.682	.345
	Concern	.502	1.000	.393	.498
	Control	.682	.393	1.000	.337
	Management	.364	.517	.358	1.000
Sig. (1-tailed)	Fatigue		<.001	<.001	<.001
	Concern	<.001		<.001	<.001
	Control	<.001	<.001		<.001
	Management	<.001	<.001	<.001	
N	Fatigue	892	892	892	892
	Concern	892	892	892	892
	Control	892	892	892	892
	Management	892	892	892	892

Multiple Linear Regression

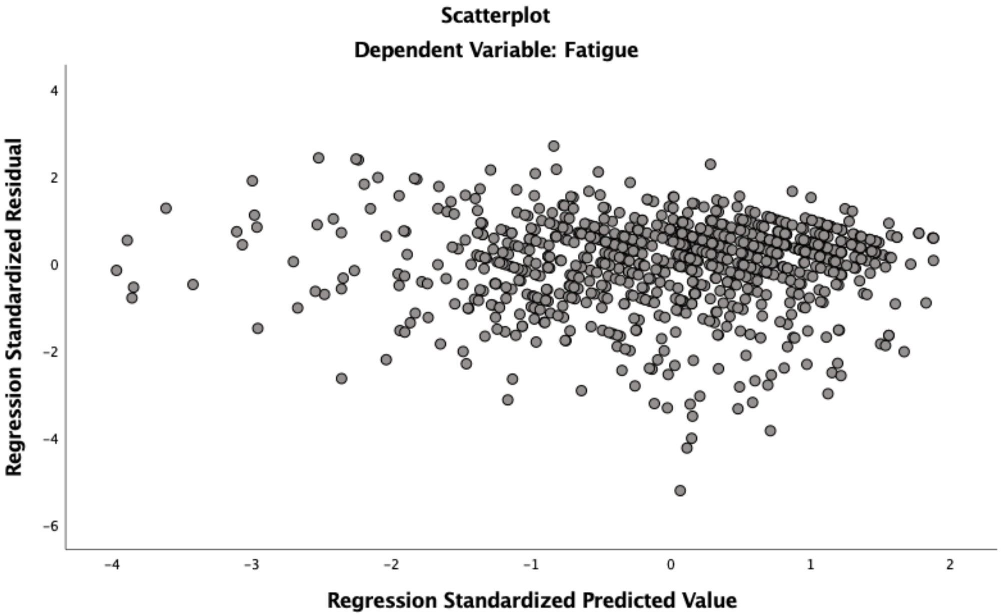
Because a strong correlation and some moderate correlations were found in the Pearson's r, a multiple regression was performed to determine the best predictor for privacy fatigue. The assumptions and results are presented below.

Assumptions

Homoscedasticity. For a linear regression, an assumption of homoscedasticity should be met. A scatterplot was used to assess the data for homoscedasticity. A visual examination shows the cigar shape that Warner (2020) noted is needed to meet the assumption.

Figure 6

Homoscedasticity for Linear Regression



Normality. The assumption of normality was assessed by visually inspecting a P-P scatterplot. For the assumption of normality to be met, the residuals must not strongly deviate from the diagonal line. Strong deviations could indicate that the parameter estimates are unreliable. Figure 7 through Figure 10 present a P-P scatterplot of the model residuals. A visual inspection of the P-P scatterplots for each variable indicates normal distribution.

Figure 7

P-P scatterplot for normality of the residuals for the regression model: Fatigue

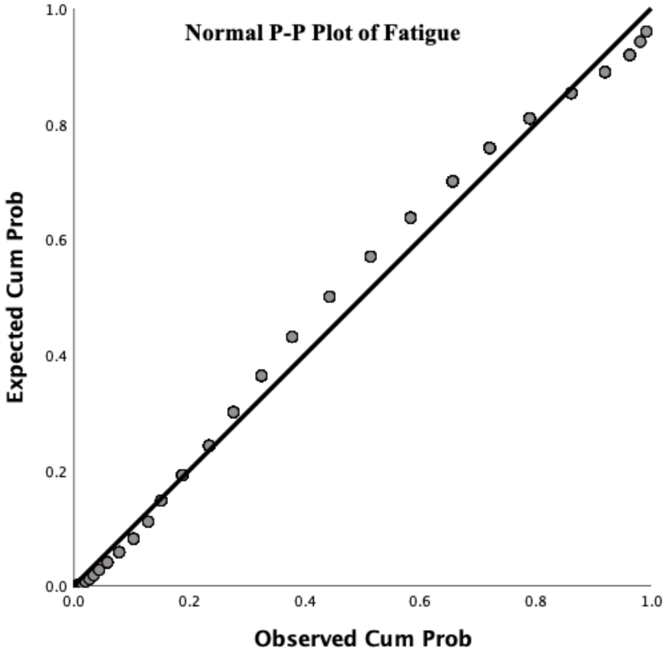


Figure 8

P-P scatterplot for normality of the residuals for the regression model: Concern

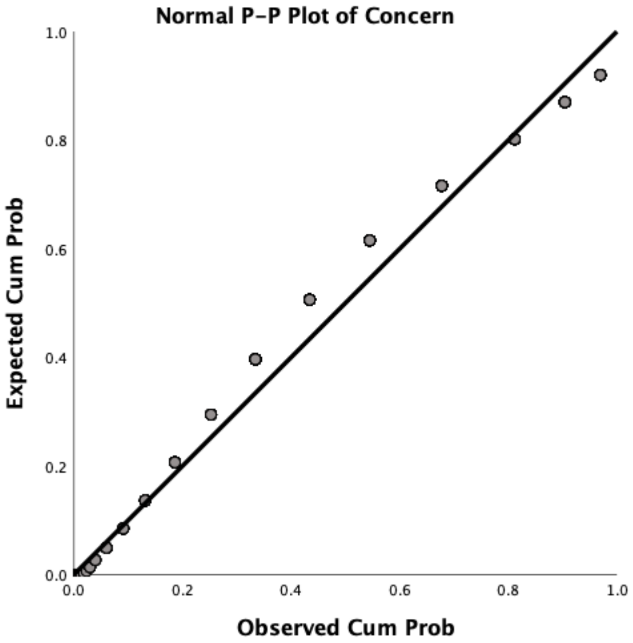


Figure 9

P-P scatterplot for normality of the residuals for the regression model: Control

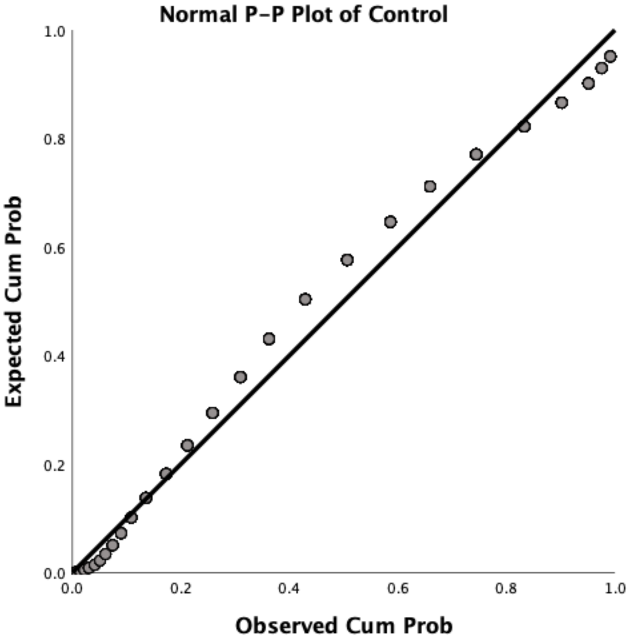
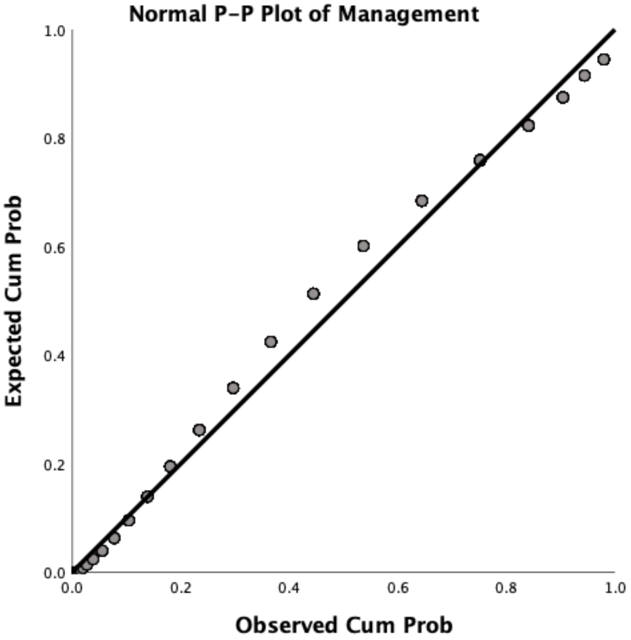


Figure 10

P-P scatterplot for normality of the residuals for the regression model: Management



Multicollinearity. Variance Inflation Factors (VIFs) were calculated to detect the presence of multicollinearity between predictors. High VIFs indicate increased effects of multicollinearity in the model. VIFs greater than 5 are cause for concern, whereas VIFs of 10 should be considered the maximum upper limit (Menard, 2009). All predictors in the regression model have VIFs less than 10. Table 13 presents the VIF for each predictor in the model.

Table 13

Variance Inflation Factors for Concern, Management, and Control

Variable	VIF
Concern	1.49
Management	1.41
Control	1.25

Results from Regression

In this regression to address the RQ, privacy concern, privacy control, and privacy management served as predictor variables and were all continuous in nature. Privacy fatigue served as the outcome variable and was also treated as continuous data. Next, an examination of the model summary table (see Table 14) reveals that the Adjusted R^2 was .528 and that 53% of variance was explained by this model. Based on this, further examination of the coefficients table was warranted. In examining Table 15, the variables of privacy concern and privacy control were found to be significant predictors of privacy fatigue. More specifically, privacy control significantly predicted privacy fatigue, B = 0.60, t(888) = 22.42, p < .001. Privacy concern significantly predicted privacy fatigue, B = 0.35, t(888) = 9.74, p < .001. Inspection of standardized beta weights showed that privacy control contributed more to the model than privacy concern. Based on this, privacy control was determined to be the largest contributor with a standard beta weight of .57, followed by privacy concern with a beta weight of .27. In addition, unstandardized beta weights show that a one-unit increase of privacy control will increase the value of privacy fatigue by .60 units, and a one-unit increase of privacy concern will increase the value of privacy fatigue by .35 units.

Table 14

Model Summary

		Model
		1
R		.738[a]
R Square		.530
Adjusted R Square		.528
Std. Error of the Estimate		.77802
Change Statistics	R Square Change	.544
	F Change	333.863
	df1	3
	df2	888
	Sig. F Change	<.001

Predictors: (Constant), Management, Control, Concern

Table 15

Coefficients

		Unstandardized	Coefficients	Standardized Coefficients		
Model		B	Std. Error	Beta	t	Sig.
1	(Constant)	-.054	.194		-.267	.789
	Concern	.345	.035	.269	9.743	<.001
	Control	.598	.027	.570	22.423	<.001
	Management	.024	.035	.019	.702	.483

Dependent Variable: Fatigue

Independent Samples *T*-Test

To address H5, two separate independent *t*-tests were performed to determine the difference in levels of privacy fatigue in females and males and the difference in levels of privacy concern in females and males. The results of the two tests are described below.

Assumptions

An assumption that must be met for an independent samples *t*-test is that there should be no significant outliers. According to Field (2018), outliers that are two or more standard deviations outside the mean must be addressed. A boxplot for privacy fatigue showed no outliers, while a boxplot for concern showed no outliers beyond two standard deviations. Two outliers within the boxplot for concern were examined and found to show no evidence of extreme answers or patterns; therefore, the two outliers were not removed. With Likert-scale data, it is important to not remove outliers that could be valid responses (Osborne & Overbay, 2008).

Privacy Fatigue in Females and Males

An independent samples *t* test was calculated to determine if there was a significant difference between the levels of privacy fatigue in females and males. Examination of group means found Females (*M* = 4.88, *SD* = 1.19) compared to Males (*M* = 5.08, *SD* = 1.09) (see Table 16). Based on this, an independent samples *t* test was performed. Examination of Levene's Test revealed that the data did violate homogeneity and that equal variances were not assumed (See Table 17). A statistically significant difference was found between the two group means (*t*(733.31) = -2.42, *p* < .05. In addition to being statistically significant, the effect size using Cohen's *d* was also calculated. The effect size was 0.2, a small effect size. H5 was not supported by the results because males statistically exhibited more fatigue than females.

Table 16

Group Statistics

	Gender	N	Mean	Std. Deviation	Std. Error Mean
Fatigue	Female	363	4.8860	1.18876	.06239
	Male	526	5.0760	1.08931	.04750

Table 17

Independent Samples Test

			Fatigue	
			Equal variances assumed	Equal variances not assumed
Levene's Test for Equality of Variances	F		4.919	
	Sig.		.027	
t-test for Equality of Means	t		-2.463	-2.424
	df		887	733.308
	Significance	One-Sided p	.007	.008
		Two-Sided p	.014	.016
	Mean Difference		-.19010	-.19010
	Std. Error Difference		.07717	.07841
	95% confidence Interval of Difference	Lower	-.34155	-.34404
		Upper	-.03864	-.03615

An independent samples *t*-test was calculated to determine if there was a significant difference between the levels of privacy concern in females and males. Examination of group means found Females (*M* = 5.1809, *SD* = .96647) compared to Males (*M* = 5.2707, *SD* = .03685) (see Table 18). Based on this, an independent samples *t* test was performed. Examination of Levene's Test revealed that the data did not violate homogeneity and that equal variances were assumed (See Table 19). A statistically significant difference was not found between the two group means (*t*(887) = -1.48, *p* = 0.07. H5 was not supported by the results because there is no significant difference in levels of concern between males and females.

Table 18

Group Statistics

	Gender	N	Mean	Std. Deviation	Std. Error Mean
Concern	Female	363	5.1887	.94049	.04936
	Male	526	5.2776	.84103	.03667

Table 19

Independent Samples Test

			Concern	
			Equal variances assumed	Equal variances not assumed
Levene's Test for Equality of Variances	F		1.732	
	Sig.		.188	
t-test for Equality of Means	t		-1.475	-1.445
	df		887	720.497
	Significance	One-Sided p	.070	.074
		Two-Sided p	.141	.149
	Mean Difference		-.08886	-.08886
	Std. Error Difference		.06025	.06149
	95% confidence Interval of Difference	Lower	-.20711	-.20959
		Upper	.02939	.03187

Summary

This study examined the digital privacy attitudes of Generation Z college students by exploring the relationship between privacy fatigue, privacy concern, privacy control, and privacy management. This chapter presented the results of statistical tests used to examine the relationship of the variables. Moderate correlations were found between privacy concern and privacy fatigue; privacy concern and privacy control; privacy concern and privacy management; privacy fatigue and privacy management; and privacy control and privacy management. A strong correlation was found between privacy fatigue and privacy control. In addition, privacy control was found to be the strongest predictor of privacy fatigue. Finally, males were found to exhibit more privacy fatigue than females, but there was no significant difference in levels of privacy concern between males and females. A discussion of the findings is presented in the following chapter.

CHAPTER FIVE: CONCLUSIONS

Overview

In 1964, McLuhan coined the term “global village” to describe how the electronic age was connecting people all over the world. Living in McLuhan’s global village of rapidly changing communication technology has made interacting in a digital environment a part of everyday communication. It can be argued that the Internet has connected and disconnected society unlike any other technology. Not only has digital technology permeated social culture but it has also created challenges when it comes to protecting personal privacy. Utilizing these digital technologies for communication cannot be avoided, particularly for younger generations. Generation Z college students engage with digital technology for not only interpersonal communication but also as an educational tool (Rospigliosi, 2019). Therefore, because digital communication is unavoidable, college students must learn to effectively navigate the many levels of privacy management strategies and boundary setting so that they feel more in control of their personal privacy. Previous research has suggested that this may aid in feeling less privacy fatigue and concern (De Wolf, 2020; Tang et al., 2020).

The purpose of this quantitative study was to explore the impact privacy fatigue, privacy concern, privacy control, and privacy management have on the digital privacy behavior of Generation Z college students within the theoretical construct of communication privacy management (CPM) theory. In this chapter, the research results are discussed and compared to previous research studies on digital privacy and CPM theory. Each research question and hypothesis are addressed within the discussion. The chapter will further present the implications of this study as well as the limitations. These are followed by recommendations for future research to encourage further knowledge of digital privacy protection behavior. Finally, a summary of the study is presented.

Discussion

This study sought to expand upon previous digital privacy research by exploring the relationship of privacy fatigue within the theoretical construct of CPM theory. The survey respondents were asked a series of 7-point Likert-type questions that focused on respondents' privacy behavior on social media. As technologies continue to rapidly develop and change, new factors must be examined as predictors of users' privacy protection behavior. Predicting communication behavior online can be difficult since there can be many influences—from cultural norms, peer pressure, and personal beliefs.

The study is situated within the sociopsychological communication tradition which posits that communication reflects a person's values and beliefs (Craig, 1999). Additionally, it describes communication as the way people interact and influence each other (Craig, 1999). Studying problems within the sociopsychological tradition of communication requires the assessment of cause and effect and appeals to the logical side of human communication (Craig, 1999). From the perspective of the sociopsychological communication tradition and through the lens of CPM theory, this study explored the cause and effect of privacy behavior within Generation Z college students.

Research Question and Hypotheses

The study was guided by a research question and six hypotheses that sought to explore the relationship between privacy fatigue, privacy concern, privacy control, and privacy management in Generation Z college students' communication on social media.

RQ: Does communication privacy management theory explain the relationship between privacy fatigue and privacy concern in Generation Z college students?

H1: Generation Z college students that exhibit a higher level of privacy concern will feel a higher level of privacy fatigue.

H2: Generation Z college students that exhibit a higher level of privacy concern feel less control over their online privacy.

H3: Generation Z college students who express a higher level of privacy concern will utilize more privacy management strategies on social media.

H4: Generation Z college students with a higher level of privacy fatigue will feel they have less control over their online privacy.

H5: Generation Z college students with a higher level of privacy fatigue will employ less online privacy management strategies.

H6: Generation Z college students who utilize more privacy management strategies will feel more control over their privacy on social media.

CPM Theory and the Impact of Privacy Fatigue and Privacy Concern

The research question focused on communication privacy management (CPM) theory and how it may address privacy fatigue and privacy concern. Initially, CPM theory was developed to predict privacy protection behavior in offline interpersonal relationships (Petronio, 2002). More recently, CPM theory has been applied to digital communication and developing boundaries and protection behavior online (De Wolf et al., 2014; Frampton & Child, 2013; Jin, 2013; Petronio & Child, 2011). CPM theory includes several key aspects; the first is that “people believe they own their own private information” (Petronio, 2002, p. 202). People feel the need to control their information so that they do not feel vulnerable (Petronio, 2002). Control and ownership are important aspects of CPM theory, and the results of this study have supported it. Statistical tests were run to find the correlation and predictors of these factors. Interestingly, privacy control was found to have the strongest correlation to privacy fatigue. In addition, privacy control was also the strongest predictor of privacy fatigue. Privacy concern had a moderate correlation and was a predictor of privacy fatigue, but it was not as strong as privacy control. Other studies have heavily focused on privacy concern as a predictor of privacy protection behavior (Baruh et al., 2017). The results from this study suggest that privacy control is a stronger predictor of privacy fatigue, connecting the factor of control within CPM theory to privacy fatigue. However, further studies into the construct of privacy fatigue are required as it is difficult to measure quantitatively; the construct needs further development and exploration.

Another key aspect of CPM theory is boundary management. People create their own boundaries to control and manage their private information. Boundaries are heavily influenced by a person’s culture, values, and belief system. The sociopsychological nature of this theory supports the claim that people are influenced by their surroundings. As people share information, they invite co-ownership of the information, forming new boundaries and expectations. When those boundaries are breached, turbulence happens. People continue in a cycle of information disclosure and privacy turbulence as a breach of boundaries is inevitable (Litt & Hargittai, 2014; Petronio, 2013). However, DeGroot and Vik (2017) suggested that privacy turbulence could be avoided or reduced by using effective privacy management strategies.

To assess CPM theory in a digital environment, the definition of boundaries is slightly different than the original definition for in-person boundaries (Metzger, 2007). The belief that one can completely control personal information online is inaccurate. There is an element of shared ownership with social media platforms as well as one’s personal network within the platform (De Wolf et al., 2014; Marwick & Boyd, 2014). The boundaries in digital communication can be more technical and complicated. However, there is one aspect that Petronio (2002) discussed that applies to both in-person and digital communication: "…when people disclose to each other, they essentially link others into a privacy boundary" (p. 203). This study assessed boundaries as privacy management strategies, such as asking about the use of privacy settings or accepting friend requests. These are only some of the ways users may enact boundaries online. According to the results, a moderate correlation was found between privacy management and concern. This suggests that privacy concern plays a role in how people enact boundaries on social media. As their level of concern increases, the more privacy management strategies they employed. Privacy concern has been proven a factor within the boundary management of CPM theory.

To further address the RQ, while CPM theory does not factor in privacy fatigue, the results of this study have shown that privacy control, a key factor in CPM theory, is a strong predictor of privacy fatigue. Therefore, this research suggests that privacy fatigue can be explained within CPM theory through the element of privacy control. In addition, privacy concern was found to be a predictor of privacy fatigue. However, it should be noted that privacy management, another key factor in CPM theory, was not a predictor of privacy fatigue. Future research should explore this relationship. In addition, as supported by previous research by De Wolf (2020), privacy concern is correlated to privacy management strategies and the boundary management aspect of CPM theory. The RQ is supported by a moderate correlation between privacy concern and privacy management, which supports previous research that found privacy concern to be a predictor of privacy management (Baruh et al., 2017).

Discussion of H1 to H5: Relationship Between Variables

In H1, it was suggested that Generation Z college students who exhibit a higher level of privacy fatigue will feel a higher level of privacy concern. With a moderate positive correlation, the results suggest that as students feel more privacy concern, it is likely that they will also feel more privacy fatigue; or the more privacy fatigue they have, the more privacy concern they will experience. In the regression, privacy concern was found to be a predictor of privacy fatigue. Therefore, in support of H1, it is suggested that Generation Z college students who experience higher levels of privacy concern will exhibit more privacy fatigue when managing their digital privacy. In their study, Xu et al. (2011) suggested that users' privacy concerns impact their perceptions and attitudes. Choi et al. (2018) and Tang et al. (2020) found privacy fatigue to be a stronger influence of privacy behavior than privacy concern. The results of this study suggest that scholars should also consider that higher privacy concern results in privacy fatigue with each playing a role in influencing privacy behavior.

In H2, it was suggested that Generation Z college students with a higher level of privacy concern will feel less control over their privacy. This hypothesis was supported by a moderate correlation between the two variables of privacy concern and privacy control. Privacy control has proven to be an important factor in influencing privacy behavior. These results support previous research which found that privacy concerns are produced when users feel a lack of control (Mosteller & Poddar, 2017; Punj, 2019). Additionally, the results of this study support previous research by Zhu and Kanjanamekanant (2021), who found that when there is a perception of co-ownership or control with social media platforms, users have less privacy concern.

In H3, it was suggested that Generation Z college students who express more privacy concern will utilize more privacy management strategies. A moderate correlation between privacy concern and privacy management was found. As privacy concern increases, privacy management strategies may also increase. This supports prior research by Trepte et al. (2020) who found that higher privacy concern resulted in the disclosure of less information. When Generation Z college students are feeling more concern about the information they share on social media, they may choose to utilize more privacy management strategies, such as restricting access to posts and personal information to friends only.

In H4, it was suggested that the more privacy fatigue Generation Z college students experienced, the less control they feel over their online privacy. In the results, privacy control showed a strong positive correlation with privacy fatigue, while the regression showed privacy control to be the strongest predictor of privacy fatigue. This suggests that when college students do not feel in control of their personal information, their level of privacy fatigue increases. Other research has found a connection between privacy control and privacy fatigue (Choi et al., 2018; De Wolf, 2020; Yang et al., 2016). Yang et al. (2016) found that users who felt they had more control over their information online were more likely to utilize social media. This result also supports the findings of Choi et al. (2018), who found that privacy fatigue is caused by a lack of privacy control. It also further demonstrates that privacy fatigue is an important factor in studying digital privacy protection behavior.

In H5, it was suggested that higher levels of privacy fatigue in Generation Z college students would result in the use of less privacy management strategies. While a moderate correlation was found between the two variables, the hypothesis was not supported because as privacy fatigue increases so do privacy management strategies. In addition, privacy management was not found to be a predictor of privacy fatigue. Therefore, in this study, privacy fatigue did not result in a lack of privacy management. However, prior research found that privacy management strategies could have an impact on college students' level of privacy fatigue. Previously, Tang et al. (2020) found that privacy fatigue impacted users' intention to disclose information. Further, when users experienced such a high level of privacy fatigue that it limited their cognitive ability, there was a decline in users' intention to protect their privacy. However, De Wolf (2020) found no relationship between personal privacy management and privacy fatigue. It has been suggested that some users do not adjust their privacy settings because they feel it will not make a difference (Masur & Trepte, 2020). This is also discussed within the results of H6.

In H6, it was suggested that Generation Z college students who utilize more privacy management strategies will feel more control over their privacy on social media. A moderate correlation was found between privacy management and privacy control. Note that in this context, the higher correlation of the variable privacy control indicates a feeling of less control. Therefore, the less control college students feel, the more they may utilize privacy management strategies. However, while a correlation was found between privacy control and privacy management, it did not support H6. Instead, the results suggest that even when using privacy management strategies on social media, the students still felt they had little control. It raises questions about what factors make college students feel more control over their personal information online. Previous research by Punj (2019) found that privacy control was a strong influencer in limiting personal information on social media, meaning more privacy management strategies were implemented. However, Punj also noted that it is not known if it is simply the perception of control or actual control measures that influence users' behavior.

Liu et al. (2017) also found that the more privacy control college students felt, the more information they disclosed. They also found that college students were more likely to adjust their privacy management settings according to what they wished to disclose. Liu et al. (2017) stated "the greatest risk to personal privacy may be the users themselves" because users voluntarily supply information on social media with their friends, family, and other acquaintances. A more thorough study of privacy control and privacy management is needed.

Discussion of H7: Gender Differences

Previous research often highlights the differences in gender in protecting privacy online. This study compared genders to see which exhibited more privacy concern and privacy fatigue. It was suggested that females exhibit more privacy concern and more privacy fatigue. However, the hypotheses were not supported. The results found that males exhibited more privacy fatigue than females. In addition, there was no significant difference found in levels of privacy concern between males and females. Metzger (2007) found that gender was not an adequate predictor of privacy concern. In contrast, De Wolf (2020) found that female teens exhibited more privacy concern than male teens. Liu et al. (2017) found that males disclosed more information and had more open privacy settings than females. If males disclose more information, that could be a factor causing them to exhibit more privacy fatigue.

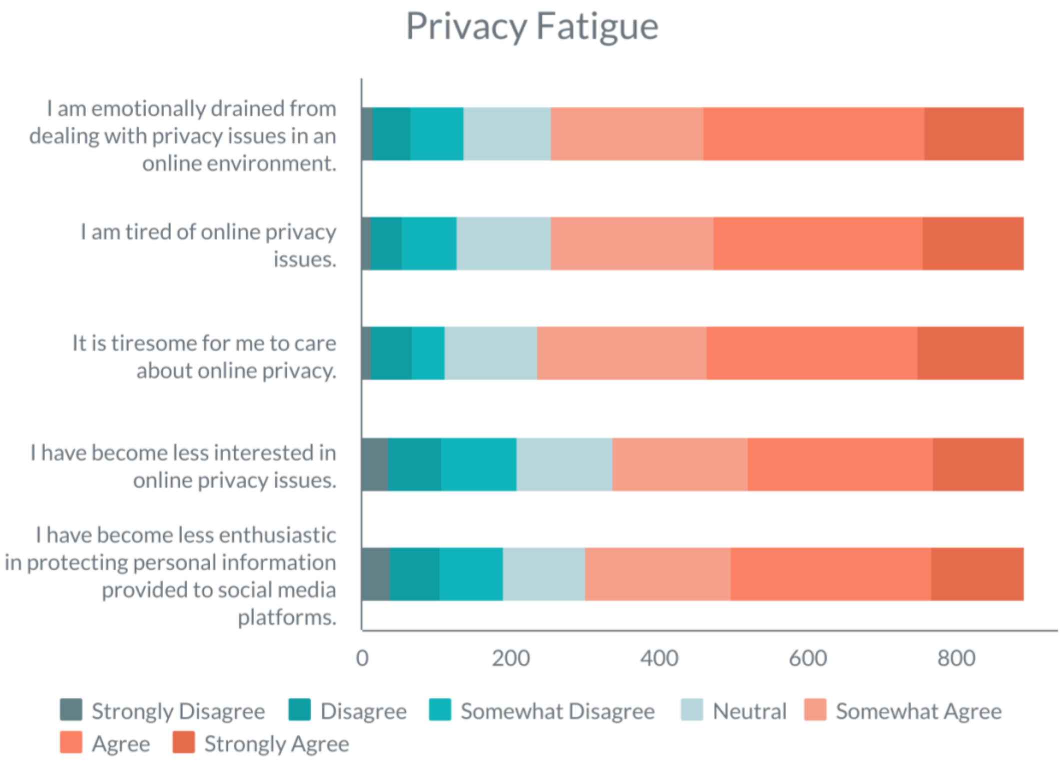
Implications

In today's world of digital communication, the Internet is the new global village. It is the environment that media technology and human interaction have created. People are instantly connected through digital technology. Social media have become not only platforms for social interaction but also a hub for cultural and political discourse (Bode, 2016). When exploring this new digital global village, people have an expectation of privacy similar to their offline activities. However, communicating online is anything but private. From third-party tracking to social media monitoring, information and communication technologies are making users vulnerable to privacy breaches.

Communicating in an online environment is something that provides fulfillment and builds relationships; it has become an integral part of everyday life. Gen Z, in particular, prefers communicating through social media and texting (Beck & Wright, 2019). However, communication in an online environment requires a different set of skills than navigating in-person communication. Even with the best intentions, users are typically communicating with a larger audience that can often be unknown because of the nature of social media and how information is shared across networks. Due to a lack of digital literacy and maturity, college students may post information that can be embarrassing or eventually damaging to their reputation or careers (Litt & Hargittai, 2014). Therefore, utilizing privacy protection behavior in digital communication is important for students to feel some control over their information. As supported by this research, privacy fatigue is a threat to effectively setting boundaries online and using privacy management strategies. The students in this study expressed a lack of control over their personal information, which has resulted in privacy fatigue—the frustrating feeling that privacy breaches are unavoidable.

Within the privacy fatigue scale on the survey, a majority of the participants answered along the agree scale—from somewhat agree to strongly agree—for each question (See Figure 11). There appears to be a high level of exhaustion and frustration over privacy issues online for Gen Z college students. Because privacy fatigue has shown to be such a strong influence on their privacy behavior, how to reduce fatigue is important to reducing students' vulnerability online. The data in this study suggests that a sense of control over personal information could reduce the feelings of privacy fatigue among Gen Z college students.

Figure 11
Privacy Fatigue Scales



This study has practical implications for organizations, such as social media platforms, apps, and online stores. Organizations can encourage more effective communication if users are given more control over how their data is utilized. Bandara et al. (2020) suggested that organizations must promote privacy empowerment—giving users control and autonomy. Often, it is difficult to navigate privacy policies and privacy settings within websites and apps. Organizations that provide user-friendly settings can help promote a safer environment for online communication. When privacy policies and settings are clearer, users may feel less fatigue when utilizing the platform. The responsibility of privacy cannot fall only on the user; organizations must also take responsibility by developing user-friendly data privacy policies. Students know that they must sacrifice some of their privacy to enjoy the benefits of online communication

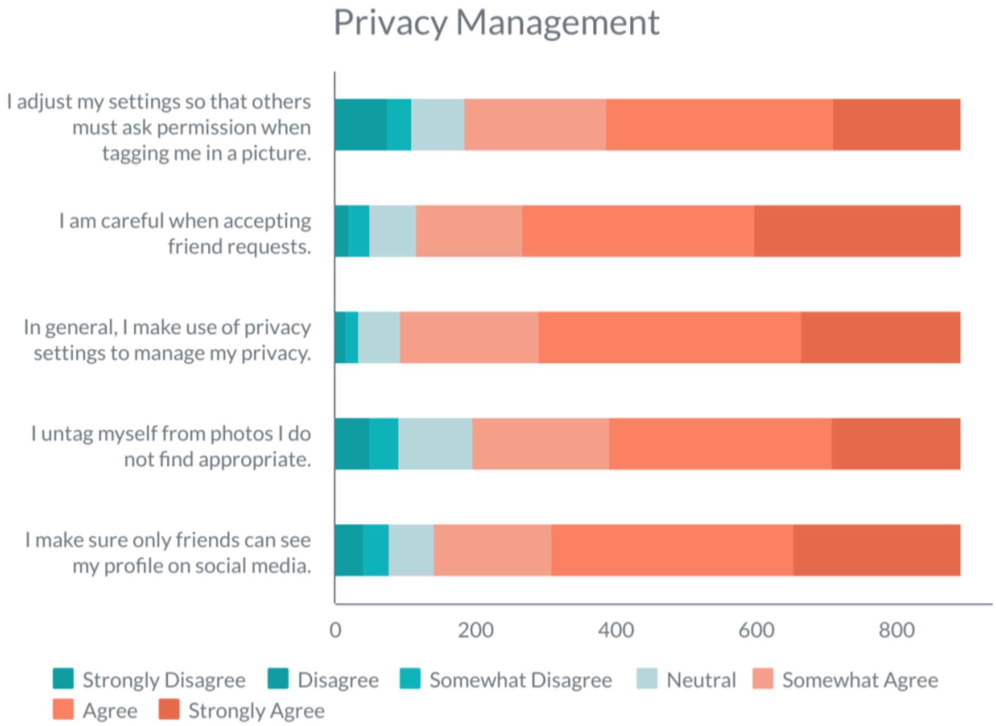
(Adorjan & Ricciardelli, 2019). However, when students feel more privacy concern and privacy fatigue, they are less likely to trust social media platforms or disclose information (Choi et al., 2018; Koohang et al., 2018). If organizations and social media platforms want to encourage more user interaction, then they must find a way to increase users' control and reduce privacy fatigue.

This study also has theoretical implications. Communication privacy management (CPM) theory does not directly address privacy fatigue within its main constructs. However, it does emphasize the construct of control. CPM theory states that people take ownership or control of their personal information (Petronio, 2002). This study supports the important factor privacy control plays in CPM theory. Additionally, the results in this study suggest that a lack of control is a strong predictor of privacy fatigue. This could help explain turbulence and boundary coordination of CPM theory. Overall, this study further supports CPM theory and its explanation of privacy control and privacy boundaries.

Further, CPM theory states that setting boundaries is an integral part of privacy management. This research asked Gen Z college students about the management strategies they use on social media. For each question, a majority of the participants answered within the agree side of the scale—from somewhat agree to strongly agree (See Figure 12). This indicates that many Gen Z college students do employ privacy management strategies. This further supports previous research that found Gen Z to be knowledgeable about privacy settings within technology (Quinn & Papacharissi, 2018). However, the use of these strategies did not appear to lower privacy concern or provide a sense of control over their personal information.

Figure 12

Privacy Management Scales



In support of CPM theory, the data from this study showed that Gen Z college students employ boundary management within their communication on social media. Additionally, the data highlighted the impact of privacy control and privacy concern on the levels of privacy fatigue shown by students. CPM theory states that people feel they own and control their personal information as well as adjust or negotiate their boundaries to protect their privacy (Petronio, 2002). The element of control within CPM theory is shown to be a significant factor for causing privacy fatigue. While total control over personal information online is not feasible, giving users better strategies may improve their digital privacy management.

Limitations

The study has several limitations. First, the sample was limited to those born between the years 1996 and 2003. This is only a subset of Generation Z, which includes those born between 1996 and 2010. It was also limited by its focus on one generation. The results of the study cannot be generalized to other age groups. Additionally, participants were recruited online within Amazon Mechanical Turk for convenience and time constraints. It gives a snapshot of that one moment in time. Running a longitudinal study may provide a more comprehensive picture of participants' attitudes.

The study is also limited by the format of the survey. An addition of yes/no or open-ended response questions could provide a more exhaustive result. Further, the questions were limited to four constructs that impact digital privacy. Other constructs, such as information disclosure and trust, could also have an impact on privacy protection behavior. Because privacy protection behavior is multifaceted, it is difficult to determine how specific factors interact and influence users. Additionally, the scales used in the survey could be refined with more statements added to improve reliability.

Recommendations for Future Research

This study sought to explore the impact of privacy fatigue on Generation Z college students' privacy protection behavior online within the theoretical construct of communication privacy management (CPM) theory. The results found privacy control to be a strong predictor of privacy fatigue. Below are recommendations to continue the study of privacy fatigue in digital communication.

Recommendation 1

Privacy fatigue has not been studied as frequently as other privacy factors like privacy concern. It has proven to be a significant factor in privacy protection behavior online. To further expand privacy fatigue research, it is recommended that a more in-depth study with mixed-methods or qualitative methodology be conducted. This would allow for a more comprehensive approach to exploring privacy fatigue and its impact on other factors within digital privacy research.

Recommendation 2

Because privacy fatigue and privacy control resulted in the strongest correlation. Further research should seek to explore the relationship between the two factors. Because communication privacy management (CPM) theory does not directly address privacy fatigue, a study focusing on privacy control and privacy fatigue could further expand the theory. Additionally, privacy control may be studied as a more significant factor than privacy concern. Future studies should consider how users can feel more in control and less fatigue when communicating in a digital environment.

Recommendation 3

Because this study focused on a subset of a specific generation, a study across generational age groups would be beneficial to assess the full impact of privacy fatigue within digital communication. Additionally, it would be beneficial to research outside of the United States for a more culturally diverse picture of privacy protection behavior.

Recommendation 4

It would be beneficial to conduct further research into privacy fatigue as a theory. Additionally, it could be explored how privacy fatigue relates to Masur's (2019) theory of situational privacy and self-disclosure and other privacy theories such as the privacy calculus theory. Further, to expand upon CPM theory, future research could focus on privacy turbulence and privacy fatigue.

Conclusion

This quantitative study sought to explore the impact of privacy fatigue, privacy concern, privacy control, and privacy management on Generation Z college students' privacy protection behavior. The research was conducted within the framework of communication privacy management (CPM) theory. A 7-point Likert-type survey was implemented to assess the attitudes of Gen Z college students. The survey contained four scales: privacy fatigue, privacy concern, privacy control, and privacy management. The results found moderate correlations among all variables and a strong correlation between privacy fatigue and privacy control. In addition, privacy control and privacy concern were found to be predictors of privacy fatigue. Privacy control was found to have the strongest correlation and to be the strongest predictor of privacy fatigue.

Because digital communication is an integral part of everyday life, the management of digital privacy will continue to be an important part of communication. In this study, Generation Z college students exhibited a high level of privacy fatigue and expressed a lack of control over their privacy. In addition, the results showed that they also had a high level of privacy concern even though they claimed to use privacy management strategies. While the other variables have been heavily researched in previous digital privacy studies, privacy fatigue is a new concept with much less previous research to support its impact. This study found privacy fatigue to be a strong influential factor in Generation Z college students' digital privacy behavior. It could explain why students show high levels of concern even when utilizing privacy management strategies. To encourage safe and effective communication, organizations and social media platforms should seek ways to increase students’ control over their personal information and reduce privacy fatigue. Further research should explore the impact of privacy fatigue within the general population.

REFERENCES

Adorjan, M., & Ricciardelli, R. (2018). *Cyber-risk and youth: Digital citizenship, privacy and surveillance*. Routledge. https://doi.org/10.4324/9781315158686

Adorjan, M., & Ricciardelli, R. (2019). A new privacy paradox? Youth agentic practices of privacy management despite “nothing to hide” online. *Canadian Review of Sociology*, *56*(1), 8–29. https://doi.org/10.1111/cars.12227

Alkire, L., Pohlmann, J., & Barnett, W. (2019). Triggers and motivators of privacy protection behavior on Facebook. *Journal of Services Marketing*, *33*(1), 57–72. https://doi.org/ 10.1108/JSM-10-2018-0287

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

Altman, I., & Taylor, D. A. (1973). *Social penetration: The development of interpersonal relationships*. Holt, Rinehart and Winston, Inc.

Anthony, D., Campos-Castillo, C., & Horne, C. (2017). Toward a sociology of privacy. *Annual Review of Sociology, 43*, 249-269. https://doi.org/10.1146/annurev-soc-060116-053643

Baik, J. (2020). Data privacy against innovation or against discrimination?: The case of the California Consumer Privacy Act (CCPA). *Telematics and Informatics, 52*. https://doi.org/10.1016/j.tele.2020.101431

Bandara, R., Fernando, M., & Akter, S. (2020). Addressing privacy predicaments in the digital marketplace: A power-relations perspective. *International Journal of Consumer Studies*, *44*(5), 423–434. https://doi.org/10.1111/ijcs.12576

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday, 11*(9). https://doi.org/10.5210/fm.v11i9.1394

Baruh, L., & Popescu, M. (2017). Big data analytics and the limits of privacy self-management. *New Media & Society*, *19*(4), 579–596. https://doi.org/10.1177/1461444815614001

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication, 67*, 26-53. https://doi.org/10.1111/jcom.12276

Beck, L. & Wright, A. (2019). iGen: What you should know about post-millennial students. *College and University, 94*(1). 21-26.

Becker, M. (2019). Privacy in the digital age: Comparing and contrasting individual versus social approaches towards privacy. *Ethics and Information Technology, 21*(4), 307-317. https://doi.org/10.1007/s10676-019-09508-z

Benjamin, G. (2017). Privacy of a cultural phenomenon. *Journal of Media Critiques*, *3*(10). https://doi.org/10.17349/jmc117204

Bergström, A., & Belfrage, M. J. (2018). News in social media: Incidental consumption and the role of opinion leaders. *Digital Journalism, 6*(5), 583-598.

Betkier, M. (2019, September). *Privacy online, law and the effective regulation of online Services*. Intersentia. https://doi.org/10.1017/9781780689371

Bode, L. (2016). Political news in the news feed: Learning politics from social media. *Mass Communication & Society, 19*(1), 24-48. https://doi.org/10.1080/15205436.2015.1045149

Boerman, S. C., Kruikemeier, S., & Borgesius, F. J. (2018). Exploring motivations for online privacy protection behavior: Insights from panel data. *Communication Research*, 1-25. https://doi.org/10.1177/0093650218800915

Boksem, M. A., Meijman, T. F., & Lorist, M. M. (2005). Efffects of mental fatigue on attention: an ERP study. *Cognitive Brain Research*, *25*(1), 107-116.

Boone, H. N., & Boone, D. A. (2012). Analyzing Likert data. *Journal of Extension, 50*(2). https://archives.joe.org/joe/2012april/pdf/JOE_v50_2tt2.pdf

Bornschein, R., Schmidt, L., & Maier, E. (2020). The effect of consumers' perceived power and risk in digital information privacy: The example of cookie notices. *Journal of Public Policy & Marketing, 39*(2), 135-154. https://doi.org/10.1177/0743915620902143

Boyle, M., & Schmierbach, M. (2020). *Applied communication research methods: Getting started as a researcher* (2nd ed.). Routledge.

Briggs, S. R., & Cheek, J. M. (1986). The role of factor analysis of the development and evaluation of personality scales. *Journal of Personality, 54,* 106-148. https://doi.org/10.1111/j.1467-6494.1986.tb00391.x

Chen, H.-T. (2018). Revisiting the privacy paradox on social media with an extended privacy calculus model: The effect of privacy concerns, privacy self-efficacy, and social capital on privacy management. *American Behavioral Scientist, 62*(10), 1392–1412. https://doi.org/10.1177/0002764218792691

Child, J. T., Petronio, S., Agyeman0Budu, E., & Westermann, D. (2011). Blog scrubbing: Exploring triggers that change privacy rules. *Computers in Human Behavior, 27*.

Choi, T. R., & Sung, Y. (2018). Instagram versus Snapchat: Self-expression and privacy concern on social media. *Telematics and Informatics, 35*(8), 2289–2298. https://doi.org/10.1016/j.tele.2018.09.009

Choon, M. J. (2018). Revisiting the privacy paradox on social media: An analysis of privacy practices associated with Facebook and Twitter. *Canadian Journal of Communication, 43*(2), 339-358. doi: 10.22230/cjc.2018v43n2a3267

Craig, R. T. (1999). Communication theory as a field. *Communication Theory, 9*(2), 119-161.

Craig, R. T. (2008). Communication in the conversation of disciplines. *Russian Journal of Communication, 1*(1), 7-23. https://doi.org/10.1080/19409419.2008.10756694

Creswell, J. W., & Creswell, J. D. (2018). *Research design: qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE.

DeGroot, J. M., & Vik, T. A. (2017). “We were not prepared to tell people yet”: Confidentiality breaches and boundary turbulence on Facebook. *Computers in Human Behavior, 70*, 351-359. http://dx.doi.org/10.1016/j.chb.2017.01.016

Dencik, L., & Cable, J. (2017). The advent of surveillance realism: Public opinion and activist responses to the Snowden leaks. *International Journal of Communication, 11*, 763-781.

Denis, D. J. (2020). *Univariate, bivariate, and multivariate statistics using R: Quantitative tools for data analysis and data science*. Wiley.

De Wolf, R. (2020). Contextualizing how teens manage personal and interpersonal privacy on social media. *New Media & Society, 22*(6), 1058-1075. https://doi.org/10.1177/1461444819876570

De Wolf, R., Willaert, K., & Pierson, J. (2014). Managing privacy boundaries together: Exploring individual and group privacy management strategies in Facebook. *Computers in Human Behavior*, *35*, 444–454. https://doi.org/10.1016/j.chb.2014.03.010

Dhir, A., Kaur, P., Chen, S., & Pallesen, S. (2019). Antecedents and consequences of social media fatigue. *International Journal of Information Management, 48*, 193-202.

Dienlin, T., & Metzger, M. J. (2016). An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative U.S. sample. *Journal of Computer-Mediated Communication*, *21*(5), 368–383. https://doi.org/10.1111/jccc4.12163

Dimock, M. (2019, January 17). Defining generations: Where millennials end and Generation Z begins. *Pew Research Center*. https://www.pewresearch.org/fact-tank/2019/01/17/where-millennials-end-and-generation-z-begins/

Dogruel, L., & Jöckel, S. (2019). Risk perception and privacy regulation preferences from a cross-cultural perspective. A qualitative study among German and U.S. smartphone users. *International Journal of Communication*, *13*, 1764-1783.

Field, A. (2018). *Discovering statistics using IBM SPSS statistics*. SAGE.

Finstad, K. (2010). Response interpolation and scale sensitivity: Evidence against 5-point scales. *Journal of Usability Studies, 5*(3), 104-110.

Fontein, D. (2019, November 13). Everything social marketers need to know about Generation Z. *Hootsuite*. https://blog.hootsuite.com/generation-z-statistics-social-marketers/

Frampton, B. D., & Child, J. T. (2013). Friend or not to friend: Coworker Facebook friend requests as an application of communication privacy management theory. *Computers in Human Behavior*, *29*(6), 2257-2264. https://doi.org/10.1016/j.chb.2013.05.006

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, *77*, 226–261. https://doi.org/10.1016/j.cose.2018.04.002

Gibbs, J. L., Ellison, N. B., & Lai, C. (2011). First comes love, and then comes Google: An investigation of uncertainty reduction strategies and self-disclosure in online dating. *Communication Research, 38*, 70-100.

Gleason, B., & von Gillern, S. (2018). Digital citizenship with social media: Participatory practices of teaching and learning in secondary education. *Educational Technology & Society, 21*(1), 200-212.

Hallam, C., & Zanella, G. (2017). Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. *Computers in Human Behavior, 68*, 217–227. https://doi.org/10.1016/j.chb.2016.11.033

Hargittai, E., & Marwick, A. (2016). "What can I really do?" Explaining the privacy paradox with online apathy. *International Journal of Communication, 10*(2016), 3737-3757.

Hart, R (2021, 12 July). WhatsApp faces EU complaint for 'aggressive' rollout of controversial privacy policies. *Forbes.* https://www.forbes.com/sites/roberthart/2021/07/12/whatsapp-faces-eu-complaint-for-aggressive-rollout-of-controversial-privacy-policies/?sh=65f3c5361a8b

Hintz, A., Dencik, L., & Wahl-Jorgensen, K. (2017). Digital citizenship and surveillance society. *International Journal of Communication, 11*(2017), 731-739.

Hunter, G. L., & Taylor, S. A. (2020). The relationship between preference for privacy and social media usage. *Journal of Consumer Marketing, 37*(1), 43–54. https://doi.org/10.1108/JCM-11-2018-2927

IBM Institute for Business Value (2017). *Uniquely Generation Z: What brands should know about today's youngest consumers*. https://glukoze.com/retail-generation-z.PDF

Jan, F., Shah, S. F., & Marwan, A. H. (2017). Testing Craig's metamodel: Shifting from classification to dimensional analysis. *The Journal of Humanities and Social Sciences, 25*(2), 13-30.

Jin, S. A. (2013). Peeling back the multiple layers of Twitter's private disclosure onion: The roles of virtual identity discrepancy and personality traits in communication privacy management on Twitter. *New Media + Society, 15*(6), 813-833. https://doi.org/10.1177/1461444812471814

Jozani, M., Ayaburi, E., Ko, M., & Choo, K.-K. R. (2020). Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective. *Computers in Human Behavior*, *107,* 106-260. https://doi.org/10.1016/j.chb.2020.106260

Kara, N. (2018). Understanding university students' thoughts and practices about digital citizenship: A mixed methods study. *Educational Technology & Society, 21*(1), 172-185.

Keith, M. J., Maynes, C., Lowery, P. B., & Babb, J. (2014). Privacy fatigue: The effect of privacy control complexity on consumer electronic information disclosure. *International Conference on Information Systems,* 14-17.

Kennedy-Lightsey, C. D., Martin, M. M., Thompson, M., Himes, K., & Clingerman, B. Z. (2012). Communication privacy management theory: Exploring coordination and ownership between friends. *Communication Quarterly, 60*(5), 665-680. https://doi.org/10.1080/01463373.2012.725004

Kim, T. (2021, April 23). Apple's privacy ad Armageddon helps familiar tech giants. *Bloomberg*. https://www.bloomberg.com/opinion/articles/2021-04-23/apple-s-new-iphone-privacy-feature-may-help-facebook-google

Koohang, A., Paliszkiewicz, J., & Goluchowski, J. (2018). Social media privacy concerns: Trusting beliefs and risk beliefs. *Industrial Management and Data Systems, 118*(6), 1209-1228. https://doi.org/10.1108/IMDS-12-2017-0558

Korolov, M. (2020, July 7). California Consumer Privacy Act (CCPA): What you need to know to be compliant. *CSO Online.* https://www.csoonline.com/article/3292578/california-consumer-privacy-act-what-you-need-to-know-to-be-compliant.html

Krauss, R. M., & Fussell, S. R. (1996). Social psychological models of interpersonal communication. In E. T. Higgins and A. Kruglanski (Eds.), *Social psychology: A handbook of basic principles* (pp. 655-701). Guilford.

Litt, E., & Hargittai, E. (2014). A bumpy ride on the information superhighway: Exploring turbulence online. *Computers in Human Behavior*, *36*, 520–529. https://doi.org/10.1016/j.chb.2014.04.027

Liu, Q., Yao, M. Z., Yang, M., & Tu, C. (2017). Predicting users' privacy boundary management strategies on Facebook. *Chinese Journal of Communication, 10*(3), 295-311. https://doi.org/10.1080/17544750.2017.1279675

Logan, K., Bright, L. F., Grau, S. L. (2018). "Unfriend me, please!": Social media fatigue and the theory of rational choice. *Journal of Marketing theory and Practice, 26*(4), 357-367. https://doi.org/10.1080/10696679.2018.1488219

Lyon, D. (2017). Surveillance culture: Engagement, exposure, and ethics in digital modernity. *International Journal of communication, 11*(2017), 824-842.

Luke, A., & Sefton-Green, J. (2018). Critical media literacy and digital ethics. *Media Development*, *3*, 6–13.

Lutz, C., Hoffmann, C. P., & Ranzini, G. (2020). Data capitalism and the user: An exploration of privacy cynicism in Germany. *New Media & Society, 22*(7), 1168-1187. https://doi.org/10.1177/1461444820912544

Madden, M., Gilman, M., Levy, K., & Marwick, A. (2017). Privacy, poverty, and big data: A matrix of vulnerabilities for poor Americans. *Washington University Law Review, 95*(1). http://openscholarship.wustl.edu/law_lawreview/vol95/iss1/6

Magolis, D., & Briggs, A. (2016). A phenomenological investigation of social networking site privacy awareness through a media literacy lens. *Journal of Media Literacy Education*, *8*(2), 22–34.

McLuhan, M. (1964). *Understanding media: The extensions of man*. Signet.

Menard, S. (2009). *Logistic regression: From introductory to advanced concepts and applications.* SAGE. https://doi.org/10.4135/9781483348964

Marron, M. B. (2015). New generations require changes beyond the digital. *Journalism & Mass Communication Educator, 70*(2), 123-124. https://doi.org/10.1177/1077695815588912

Marwick, A. E., & Boyd, D. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society, 16*(7), 1051-1067. https://doi.org/10.1177/1461444814543995

Masur, P. K. (2019). *Situational privacy and self-disclosure: Communication Processes in Online Environments*. Springer.

Masur, P. K., Teutsch, D., Trepte, S., (2017). Development and validation of online privacy competence scale (OPLIS). *Diagnostica, 63*(4), 256-269. https://doi.org/10.1025/0012-1924/a000179

Masur, P. K., & Trepte, S. (2020). Transformative or not? How privacy violation experiences influence online privacy concerns and online information disclosure. *Human Communication Research,* 1-26. https://doi.org/10.1093/hcr/hqaa012

Mathew, W. (2020, January 24). Marketing to millennials and Generation Z: Things are changing. *The Drum*. https://www.thedrum.com/opinion/2020/01/24/marketing-millennials-and-generation-z-things-are-changing

Matjasic, M., Vehovar, V., & Manfreda, K. L. (2018). Web survey paradata on response time outliers: A systematic literature review. *Advances in Methodology and Statistics, 15*(1), 23-41. https://ibmi.mf.uni-lj.si/mz/2018/no-1/Matjasic2018.pdf

Metzger, M. J. (2007). Communication privacy management in electronic commerce. *Journal of Computer-Mediated Communication, 12,* 335-361. https://doi.org/10.1111/j.1083-6101.2007.00328.x

Mossberger, K., Tolbert, C. J., & McNeal, R. S. (2008). *Digital citizenship: The Internet, society, and participation*. MIT Press.

Mosteller, J., & Poddar, A. (2017). To share and protect: Using regulatory focus theory to examine the privacy paradox of consumers' social media engagement and online privacy protection behaviors. *Journal of Interactive Marketing*, *39*, 27–38. https://doi.org/10.1016/j.intmar.2017.02.003

Norman, G. (2010). Likert scales, levels of measurement and the "laws" of statistics. *Advances in Health Science Education, 15*(5), 625-632. https://doi.org/10.1007/s10459-010-9222-y

Nuzulita, N., & Subriadi, A. P. (2019). The role of risk-benefit and privacy analysis to understand different uses of social media by Generations X, Y, and Z in Indonesia. *The Electronic Journal of Information Systems in Developing Countries*. https://doi.org/10.1002/isd2.12122

Obar, J. (2019). Searching for data privacy self-management: Individual data control and Canada's digital strategy. *Canadian Journal of Communication, 44*(2). https://doi.org/10.22230/cjc.2019v44n2a3503

Office of the United Nations High Commissioner for Human Rights. (1966). *International covenant on political and civil rights.* Retrieved from https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

Office of the United Nations High Commissioner for Human Rights. (n.d.). *The right to privacy in the digital age.* Retrieved from https://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx

Osborne, J. W., & Overbay, A. (2008). Best practices in data cleaning: How outliers and “fringeliers” can increase error rates and decrease the quality and precision of your results. In J. W. Osborne (Ed.), *Best practices in quantitative methods* (205-213). SAGE.

Pallant, J. (2010). *SPSS survival manual.* McGraw Hill.

Park, Y. J. (2011). Digital literacy and privacy behavior online. *Communication Research*, *40*(2), 215–236. https://doi.org/10.1177/0093650211418338

Parker, K., & Igielnik, R. (2020). On the cusp of adulthood and facing an uncertain future: What we know about Gen Z so far. *Pew Research Center*. https://www.pewresearch.org/social-trends/2020/05/14/on-the-cusp-of-adulthood-and-facing-an-uncertain-future-what-we-know-about-gen-z-so-far-2/

Petronio, S. (1991). Communication boundary management: A theoretical model of managing disclosure of private information between marital couples. *Communication Theory, 1*, 311-335.

Petronio, S. (1994). Privacy binds in family interactions: The case of parental privacy invasion. In W.R. Cupach & B. H. Spitzberg (Eds.). *LEA’s communication series. The dark side of interpersonal communication* (p. 241-257). Lawrence Erlbaum Associates, Inc.

Petronio, S. (2002). *Boundaries of Privacy: Dialectics of Disclosure*. SUNY Press.

Petronio, S. (2013). Brief status report on communication privacy management theory. *Journal of Family Communication, 13*(1), 6-14. https://doi.org/10.1080/15267431.2013.743426

Petronio, S. & Child, J. T. (2011). Unpacking the paradoxes of privacy in CMC relationships: The challenges of blogging and relational communication on the Internet. In K. B. Wright, L. M. Webb (Eds.), *Computer-mediated communication in personal relationships*. Hampton Press.

Petronio, S., & Child, J. T. (2020). Conceptualization and operationalization: Utility of communication privacy management theory. *Current Opinion in Psychology*, *31*, 76–82. https://doi.org/10.1016/j.copsyc.2019.08.009

Petronio, S., & Martin, J. N. (1986). Ramifications of revealing private information: A gender gap. *Journal of Clinical Psychology, 42*(3), 499-506. https://doi.org/10.1002/1097-4679(198605)42:3<499::AID-JCLP2270420317>3.0.CO;2-I

Pew Research Center. (2019, November 15). Americans and Privacy: Concerned, confused and feeling lack of control over their personal information. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Pew Research Center (2021, April 7). *Social media fact sheet.* https://www.pewresearch.org/internet/fact-sheet/social-media/

Priporas, C., Stylos, N., Fotiadis, A. K. (2017). Generation Z consumers' expectations of interactions in smart retailing: A future agenda. *Computer in Human Behavior*, *77*, 374-381. https://doi.org/10.1016/j.chb.2017.01.058

Pritchard, I. (2011). How do IRB members make decisions? A review and research agenda. *Journal of empirical research on human research ethics, 6*(2). 31-46.

https://doi.org/10.1525/jer.2011.6.2.31

Puiu, S. (2016). Generation Z -- a new type of consumers. *Young Economists Journal 13*(27), 67–78.

Punj, G. N. (2019). Understanding individuals' intentions to limit online personal information disclosures to protect their privacy: Implications for organizations and public policy. *Information Technology and Management*, *20*(3), 139–151. https://doi.org/10.1007/s10799-018-0295-2

Quinn, K., & Papacharissi, Z. (2018). The contextual accomplishment of privacy. *International Journal of Communication 12*, 45-67.

Ravindran, T., Kuan, A. C., Lian, D. G. (2014). Antecedents and effects of social network fatigue. *Journal of the Association for Information Science and Technology, 65*(11), 2306-2320. https://doi-org.ezproxy.liberty.edu/10.1002/asi.23122

Rospigliosi, P. (2019). The role of social media as a learning environment in the fully functioning university: Preparing for Generation Z. *Interactive Learning Environments, 27*(4), 429-431. https://doi.org/10.1080/10494820.2019.1601849

Seemiller, C., & Grace, M. (2019). *Generation Z: A century in the making*. Routledge.

Sheehan, K. B. (2018). Crowdsourcing research: Data collection with Amazon's Mechanical Turk. *Communication Monographs, 85*(1), 140-156. https://doi.org/10.1080/03637751.2017.1342043

Sindermann, C., Schmitt, H. S., Kargl, F., Herbert, C., & Montag, C. (2021). Online privacy literacy and online privacy behavior—The role of crystallized intelligence and personality. *International Journal of Human-Computer Interaction,* 1-12. https://doi.org/10.1080/10447318.2021.1894799

Statista Research Department. (2021, January 20). U.S. population by generation 2019. https://www.statista.com/statistics/797321/us-population-by-generation/

Subedi, B. P. (2016). Using Likert type data in social science research: Confusion, issues, and challenges. *International Journal of Cotemporary Applied Sciences, 3*(2), 36-49. http://www.ijcar.net/assets/pdf/Vol3-No2-February2016/02.pdf

Tang, J., Akram, U., & Shi, W. (2020). Why people need privacy? The role of privacy fatigue in app users' intention to disclose privacy based on personality traits. *Journal of Enterprise Information Management.* https://doi.org/10.1108/JEIM-03-2020-0088

Trepte, S. (2015). Social media, privacy, and self-disclosure: The turbulence caused by social media's affordances. *Social Media + Society,* 1-2. https://doi.org/10.1177/ 2056305115578681

Trepte, S. (2020). The social media privacy model: Privacy and communication in the light of social media affordances. *Communication Theory*, 1-22. https://doi.org/10.1093/ct/qtz035

Trepte, S., Scharkow, M., & Dienlin, T. (2020). The privacy calculus contextualized: The influence of affordances. *Computers in Human Behavior,* 104. https://doi.org/10.1016/j.chb.2019.08.022

Trepte, S., Teutsch, D., Masur, P K., Eicher, C., Fischer, M., Hennhofer, A., & Lind, F. (2015). Do people know about privacy and data protection strategies? Towards the "online privacy literacy scale" (OPLIS). In S. Guwirth, R. Leenes, & P. de Hert (Eds.), *Reforming European data protection law* (Vol. 20). Springer.

Turner, A. (2015). Generation Z: Technology and social interest. *Journal of Individual Psychology, 71*(2), 103-113.

Twenge, J. M. (2017). *IGen: Why today's super-connected kids are growing up less rebellious,* *more tolerant, less happy—And completely unprepared for adulthood—And what that means for the rest of us*. Atria Books.

Vehovar, V., & Manfreda, K. L. (2017). Overview: Online surveys. In N. G. Fielding, L. M. Raymond, & G. Blank (Eds.), *The SAGE Handbook of Online Research Methods*. SAGE https://dx.doi.org/10.4135/9781473957992

Warner, R. (2020). *Applied statistics: From bivariate through multivariate techniques* (3rd ed.). SAGE.

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

Waters, S., & Ackerman, J. (2011). Exploring privacy management on Facebook: Motivations and perceived consequences of voluntary disclosure. *Journal of Computer-Mediated Communication, 17*, 101-115.

Westin, A. F. (1970). *Privacy and freedom* (6th ed.).

Atheneum.

Wisniewski, P. J., Knijnenburg, B. P., & Lipford, H. R. (2017). Making privacy personal: Profiling social network users to inform privacy education and nudging. *International Journal of Human-Computer Studies, 98*, 95-108. http://dx.doi.org/10.1016/j.ijhcs.2016.09.006

Wood, S. (2013). Generation Z as Consumers: Trends and Innovation. *Institute for Emerging Issues*. https://iei.ncsu.edu/wp-content/uploads/2013/01/GenZConsumers.pdf

Wrench, J. S., Thomas-Maddox, C., McCroskey, J. C., & Richmond, V. P. (2019). *Quantitative research methods for communication: A hands-on approach* (4th ed.). Oxford University Press.

Xie, W., & Karan, K. (2019). Consumers' privacy concern and privacy protection on social network sites in the era of big data: Empirical evidence from college students. *Journal of Interactive Advertising*, *19*(3), 187–201. https://doi.org/10.1080/15252019.2019.1651681

Xu, H., Dinev, T., Smith, J., Hart, P. (2011). Information privacy concerns: Linking individual perceptions with the institutional privacy assurances. *Journal of the Association of Information Systems, 12*(12), 798-824.

Xu, S., Yang, H. H., MacLeod, J., & Zhu, S. (2019). Social media competence and digital citizenship among college students. *Convergence*, *25*(4), 735–752. https://doi.org/10.1177/1354856517751390

Yan, T. (2008). Nondifferentiation. In P. J. Lavrakas (Ed.), *Encyclopedia of survey research methods.* SAGE.

Yang, K. C., & Kang, Y. (2015). Exploring big data and privacy in strategic communication campaigns: A cross-cultural study of mobile social media users' daily experiences. *International Journal of Strategic Communication, 9*(2), 87-101. https://doi.org/10.1080/1553118X.2015.1008635

Yang, K. C., Pulido, A., & Kang, Y. (2016). Exploring the relationship between privacy concerns and social media use among college students: A communication privacy management perspective. *Intercultural Communication Studies, 25*(2), 46-62.

Yerby, J., Koohang, A., & Paliszkiewicz, J. (2019). Social media privacy concerns and risk beliefs. *Online Journal of Applied Knowledge Management (OJAKM), 7*(1), 1–13. https://doi.org/10.36965/OJAKM.2019.7(1)1-13

Yu, A., Nekmat, E., & Beta, A. R. (2019). Digital literacy through digital citizenship: Online civic participation and public opinion evaluation of youth minorities in Southeast Asia. *Media and Communication, 7*(2), 100-114. https://doi.org/10.17645/mac.v7i2.1899

Zhu, Y., & Bao, Z. (2018). The role of negative network externalities in SNS fatigue: An empirical study based on impression management concern, privacy concern, and social overload. *Data Technologies and Applications, 52*(3).

Zhu, Y., & Kanjanamekanant, K. (2021). No trespassing: Exploring privacy boundaries in personalized advertisement and its effects on ad attitude and purchase intentions on social media. *Information & Management*, *58*(2). https://doi.org/10.1016/j.im.2020.103314

APPENDIX

Survey

Consent

Title of the Project: Digital Privacy: Generation Z and the Influence of Privacy Fatigue

Principal Investigator: Sara Allison Brake, Liberty University

Invitation to be Part of a Research Study: You are invited to participate in a research study. To participate, you must be between ages 18-25 and be in enrolled in or have complete college-level courses. Taking part in this research project is voluntary. Please take time to read this entire form and ask questions before deciding whether to take part in this research.

What is the study about and why is it being done? The purpose of the study is to explore how Generation Z college students protect their online privacy on social media. Additionally, the study seeks to better understand how Generation Z college students manage privacy fatigue online.

What will happen if you take part in this study? If you agree to be in this study, I will ask you to complete an anonymous online survey that will take less than 10 minutes.

How could you or others benefit from this study? Participants should not expect to receive a direct benefit from taking part in this study. Benefits to society include a better understanding of how Generation Z college students manage their privacy online. It may also provide insights into how organizations can provide better privacy practices to encourage safe and effective online communication.

What risks might you experience from being in this study? The risks involved in this study are minimal, which means they are equal to the risks you would encounter in everyday life.

How will personal information be protected? The records of this study will be kept private.

Research records will be stored securely, and only the researcher will have access to the records. Participant responses will be anonymous. Data will be stored on a password-locked computer and may be used in future presentations. After three years, all electronic records will be deleted.

Is study participation voluntary? Participation in this study is voluntary. Your decision whether to participate will not affect your current or future relations with Liberty University. If you decide to participate, you are free to not answer any question or withdraw at any time prior to submitting the survey. If you choose to withdraw from the study, please exit the survey and close your Internet browser. Your responses will not be recorded or included in the study.

What should you do if you decide to withdraw from the study? If you choose to withdraw from the study, please exit the survey and close your Internet browser.

Whom do you contact if you have questions or concerns about the study? The researcher conducting this study is Sara Allison Brake. You may ask any questions you have now. If you have questions later, you are encouraged to contact her at ___________. You may also contact the researcher's faculty sponsor, Dr. Tabitha Cassidy, at ___________.

Whom do you contact if you have questions about your rights as a research participant? If you have any questions or concerns regarding this study and would like to talk to someone other than the researcher, you are encouraged to contact the Institutional Review Board, 1971 University Blvd., Green Hall Ste. 2845, Lynchburg, VA 24515 or email at irb@liberty.edu.

Disclaimer: The Institutional Review Board (IRB) is tasked with ensuring that human subjects research will be conducted in an ethical manner as defined and required by federal regulations. The topics covered and viewpoints expressed or alluded to by student and faculty researchers are those of the researcher and do not necessarily relect the official policies or positions of Liberty University.

Do you agree to the above terms? By clicking "yes" below, you consent that you are willing to answer the questions in the survey.

1. What is your gender?
   - ○ Male
   - ○ Female
   - ○ Other
2. Please enter your age: ___
3. What is the highest degree or level of school you have completed?
   - ○ High School Degree or Equivalent (e.g., GED)
   - ○ Trade School
   - ○ Currently Enrolled in College
   - ○ Associate Degree
   - ○ Bachelor’s Degree
   - ○ Master’s Degree

For the following questions, please choose the answer that most applies to you:

4. I am concerned that the information I submit to online social media platforms could be misused.
   - ○ Strongly Agree
   - ○ Agree
   - ○ Somewhat Agree
   - ○ Neither Agree or Disagree
   - ○ Somewhat Disagree
   - ○ Disagree

- ○ Strongly Disagree

5. I am concerned that a person can find private information about me on the Internet.
   - ○ Strongly Agree
   - ○ Agree
   - ○ Somewhat Agree
   - ○ Neither Agree or Disagree
   - ○ Somewhat Disagree
   - ○ Disagree
   - ○ Strongly Disagree
6. I am concerned that others will post embarrassing information about me on social media.
   - ○ Strongly Agree
   - ○ Agree
   - ○ Somewhat agree
   - ○ Neither Agree or Disagree
   - ○ Somewhat Disagree
   - ○ Disagree
   - ○ Strongly Disagree
7. I am concerned about providing personal information to social media platforms because it could be used in a way I did not foresee.
   - ○ Strongly Agree
   - ○ Agree
   - ○ Somewhat Agree
   - ○ Neither Agree or Disagree

- ○ Somewhat Disagree
- ○ Disagree
- ○ Strongly Disagree

8. I feel emotionally drained from dealing with privacy issues in an online environment.
    - ○ Strongly Agree
    - ○ Agree
    - ○ Somewhat Agree
    - ○ Neither Agree or Disagree
    - ○ Somewhat Disagree
    - ○ Disagree
    - ○ Strongly Disagree
9. I am tired of online privacy issues.
    - ○ Strongly Agree
    - ○ Agree
    - ○ Somewhat Agree
    - ○ Neither Agree or Disagree
    - ○ Somewhat Disagree
    - ○ Disagree
    - ○ Strongly Disagree
10. It is tiresome for me to care about online privacy.
    - ○ Strongly Agree
    - ○ Agree
    - ○ Somewhat Agree

- ○ Neither Agree or Disagree
- ○ Somewhat Disagree
- ○ Disagree
- ○ Strongly Disagree

11. I have become less interested in online privacy issues.

    - ○ Strongly Agree
    - ○ Agree
    - ○ Somewhat Agree
    - ○ Neither Agree or Disagree
    - ○ Somewhat Disagree
    - ○ Disagree
    - ○ Strongly Disagree

12. I have become less enthusiastic in protecting personal information provided to social media platforms.

    - ○ Strongly Agree
    - ○ Agree
    - ○ Somewhat Agree
    - ○ Neither Agree or Disagree
    - ○ Somewhat Disagree
    - ○ Disagree
    - ○ Strongly Disagree

13. I have little control over online privacy.

    - ○ Strongly Agree

- Agree
- Somewhat Agree
- Neither Agree or Disagree
- Somewhat Disagree
- Disagree
- Strongly Disagree

14. Adjusting my personal privacy settings has little impact.

- Strongly Agree
- Disagree
- Somewhat Disagree
- Neither Agree or Disagree
- Somewhat Disagree
- Disagree
- Strongly Disagree

15. It is impossible, as an individual, to control my personal information by myself.

- Strongly Agree
- Agree
- Somewhat Agree
- Neither Agree or Disagree
- Somewhat Disagree
- Disagree
- Strongly Disagree

16. It is impossible to control who shares information about me.

- ○ Strongly Agree
- ○ Agree
- ○ Somewhat Agree
- ○ Neither Agree or Disagree
- ○ Somewhat Disagree
- ○ Disagree
- ○ Strongly Disagree

17. In general, I have the feeling that I can exert little control over my personal information.

- ○ Strongly Agree
- ○ Agree
- ○ Somewhat Agree
- ○ Neither Agree or Disagree
- ○ Somewhat Disagree
- ○ Disagree
- ○ Strongly Disagree

18. I adjusted my settings so that others must ask permission when tagging me in a picture.

- ○ Strongly Agree
- ○ Agree
- ○ Somewhat Agree
- ○ Neither Agree or Disagree
- ○ Somewhat Disagree
- ○ Disagree
- ○ Strongly Disagree

19. I am careful when accepting friend requests.

○ Strongly Agree

○ Agree

○ Somewhat Agree

○ Neither Agree or Disagree

○ Somewhat Disagree

○ Disagree

○ Strongly Disagree

20. In general, I make use of privacy settings to manage my privacy.

○ Strongly Agree

○ Agree

○ Somewhat Agree

○ Neither Agree or Disagree

○ Somewhat Disagree

○ Disagree

○ Strongly Disagree

21. I untag myself from photos I do not find appropriate.

○ Strongly Agree

○ Agree

○ Somewhat Agree

○ Neither Agree or Disagree

○ Somewhat Disagree

○ Disagree

- Strongly Disagree

22. I make sure only friends can see my profile on social media.

  - Strongly Agree
  - Agree
  - Somewhat Agree
  - Neither Agree or Disagree
  - Somewhat Disagree
  - Disagree
  - Strongly Disagree

23. What device do you use most often to access social media?

  - Smartphone
  - Tablet
  - Laptop Computer
  - Desktop Computer
  - Other

24. Which platform do you use?

  - iOS
  - Android
  - Other

25. Which race/ethnicity best describes you? (Please choose only one.)

  - White/Caucasian
  - Black/African American
  - Latino/Hispanic

- ○ Asian
- ○ Native American
- ○ Native Hawaiian or Pacific Islander
- ○ Other

26. If applicable, please specify your religion.

- ○ Christian
- ○ Catholic
- ○ Jewish
- ○ Muslim
- ○ Buddhist
- ○ Hindu
- ○ Atheist
- ○ Agnostic
- ○ Prefer not to say

27. What is your political viewpoint?

- ○ Very conservative
- ○ Slightly conservative
- ○ Neutral/Neither conservative or liberal
- ○ Slightly Liberal
- ○ Very liberal
- ○ I prefer not to say