




2021

THE CONSENT OF MAN: AN EXAMINATION OF PRIVACY AWARENESS, SURVEILLANCE, AND PRIVACY POLICY (MIS)USE

Will Reilley Silberman

University of Kentucky, wrsi227@g.uky.edu

Author ORCID Identifier:

 <https://orcid.org/0000-0001-9040-1964>

Digital Object Identifier: <https://doi.org/10.13023/etd.2021.161>

[Right click to open a feedback form in a new tab to let us know how this document benefits you.](#)

Recommended Citation

Silberman, Will Reilley, "THE CONSENT OF MAN: AN EXAMINATION OF PRIVACY AWARENESS, SURVEILLANCE, AND PRIVACY POLICY (MIS)USE" (2021). *Theses and Dissertations--Communication*. 104.

https://uknowledge.uky.edu/comm_etds/104

This Doctoral Dissertation is brought to you for free and open access by the Communication at UKnowledge. It has been accepted for inclusion in Theses and Dissertations--Communication by an authorized administrator of UKnowledge. For more information, please contact UKnowledge@lsv.uky.edu.

STUDENT AGREEMENT:

I represent that my thesis or dissertation and abstract are my original work. Proper attribution has been given to all outside sources. I understand that I am solely responsible for obtaining any needed copyright permissions. I have obtained needed written permission statement(s) from the owner(s) of each third-party copyrighted matter to be included in my work, allowing electronic distribution (if such use is not permitted by the fair use doctrine) which will be submitted to UKnowledge as Additional File.

I hereby grant to The University of Kentucky and its agents the irrevocable, non-exclusive, and royalty-free license to archive and make accessible my work in whole or in part in all forms of media, now or hereafter known. I agree that the document mentioned above may be made available immediately for worldwide access unless an embargo applies.

I retain all other ownership rights to the copyright of my work. I also retain the right to use in future works (such as articles or books) all or part of my work. I understand that I am free to register the copyright to my work.

REVIEW, APPROVAL AND ACCEPTANCE

The document mentioned above has been reviewed and accepted by the student's advisor, on behalf of the advisory committee, and by the Director of Graduate Studies (DGS), on behalf of the program; we verify that this is the final, approved version of the student's thesis including all changes required by the advisory committee. The undersigned agree to abide by the statements above.

Will Reilley Silberman, Student

Dr. Anthony Limperos, Major Professor

Dr. Anthony Limperos, Director of Graduate Studies

THE CONSENT OF MAN: AN EXAMINATION OF PRIVACY AWARENESS,
SURVEILLANCE, AND PRIVACY POLICY (MIS)USE

DISSERTATION

A dissertation submitted in partial fulfillment of the
requirements for the degree of Doctor of Philosophy in the
College of Communication and Information
at the University of Kentucky

By
Will Reilley Silberman
Lexington, Kentucky
Director: Dr. Anthony Limperos, Associate Professor of Communication
Lexington, Kentucky
2021

Copyright © Will Reilley Silberman 2021
<https://orcid.org/0000-0001-9040-1964>

ABSTRACT OF DISSERTATION

THE CONSENT OF MAN: AN EXAMINATION OF PRIVACY AWARENESS, SURVEILLANCE, AND PRIVACY POLICY (MIS)USE

The problem of privacy is nuanced, pervasive, and requires an elevated approach. Given the lack of consistency with regard to privacy's conceptualization and operationalization, research is needed that examines variables related to privacy to better understand how privacy operates in the present day. This dissertation aims to better understand nuances of privacy by gauging knowledge of online privacy, technological affordances related to privacy, and knowledge of surveillance. In this study, human subjects from a large southern University were presented with an opportunity to use a privacy-invasive smartphone application. After doing so, they viewed one of three privacy policies. Finally, they answered survey items measuring privacy awareness and surveillance awareness.

It was found that there were no significant main effects between modality of privacy policy shown and awareness of privacy nor awareness of surveillance. However, significant individual differences were found between two types of privacy policies. It was also found that a significant and positive relationship existed between awareness of privacy, and awareness of surveillance. It was also found that a relationship existed between awareness of privacy and awareness of the communication affordances of visibility and encryption. The present study concludes with implications that benefit communication theory, social media research, and legal bodies who seek to address issues with present day privacy policies.

KEYWORDS: Privacy, Surveillance, Affordances, Privacy Policies, Privacy Paradox

Will Reilley Silberman

(Name of Student)

04/29/2021

Date

THE CONSENT OF MAN: AN EXAMINATION OF PRIVACY AWARENESS,
SURVEILLANCE, AND PRIVACY POLICY (MIS)USE

By
Will Reilley Silberman

Anthony Limperos

Director of Dissertation

Anthony Limperos

Director of Graduate Studies

04/29/2021

Date

DEDICATION

There are good men, there are bad men, and there are... *Silbermen*. This dissertation in all of its caffeinated glory, is dedicated in honor of, and to, Jeff Silberman and his legacy.

My father was a man of too many, yet too little, words, yet not enough can be said to describe how much I miss you, your wisdom, and your dry sense of humor. I sincerely wish that you could read this dissertation...just so you can call me a putz once more.

May you rest in power, Jeffy.

ACKNOWLEDGMENTS

The following caffeinated dissertation, while an individual work, benefited from the insights and direction of several people. I would first like to acknowledge my Dissertation Chair and Advisor, Anthony Limperos, for his continued support, guidance, and knowledge throughout this entire doctoral process. Outside of the dissertation, Anthony became family in that he opened his house, family, and life to support me and my quest to obtain a PhD. I am eternally grateful for his patience. Next, I wish to thank my complete Comprehensive Examination and Dissertation Committee, and outside reader, respectively: Jeannette Sutton, Sherali Zeadally, Kenneth Calvert, and John Nash. At every milestone, be it the literature collection, examination preparation, examination evaluation, proposal, and beyond, my committee supported my research endeavors and offered nothing but avenues of improvement for me to turn my work into something worthy of review and sharing with the academy. I am thankful for your insights, and I am so glad to have worked with you.

Outside of the technical and instrumental doctoral assistance above, I received equally important assistance from family and friends. My Knight, Cody, was here for me when I felt the immeasurable doctoral pressure and weight of decaffeination as I proceeded through the program. I am eternally thankful for your love, warmth, and patience as I went from “Mr. PhD” to... “Dr. Will.” My wifey, Britt, for being the best wifey and supporting me as you slayed your law degree and became a superstar lawyer in multiple states; I love you so *mitch!* My family: Barbara, Scott, Rochelle, Grandma, Yia Yia, Diane, Chrissy, Denise, Jamie, TJ, Phil, Brent, and Marlee. My colleagues and advisors at San Diego State: Brian Spitzberg and Rachael Record. My friends here at the

University of Kentucky: Dr. Don Lowe (my Galentina), Amanda, Sarah, Erin, Sean, Alexis, Meredith, Lauren, Ted, Nathan, and Elizabeth. My friends outside of Kentucky: Bryan, Mumin, Colin, Hannah, Joel, Tahil, Jaz, and Mary Anne. My colleagues and friends in the debate community: Gina, Rob M., John, Rob R., Steve, Dave, Rebecca, Ian and Tuna. I wish to thank the respondents of my study (who remain anonymous in compliance with the IRB's recommendations to preserve their privacy). Finally, it would behoove me to recognize and thank Dr. Anthony Fauci. The COVID-19 pandemic put the health and livelihood of the nation on the line. Acting as the voice and defender of science is a thankless job; I am eternally thankful for your bravery in preparing the world to overcome COVID-19.

TABLE OF CONTENTS

ACKNOWLEDGMENTS.....	iii
LIST OF TABLES	vii
CHAPTER 1. INTRODUCTION.....	1
1.1 <i>The Problem of Privacy</i>	1
CHAPTER 2. LITERATURE REVIEW, HYPOTHESES, AND RESEARCH QUESTIONS	4
2.1 <i>Overview</i>	4
2.2 <i>On Defining (and Theorizing) a Theory of Privacy</i>	4
2.3 <i>Privacy in Alternative Settings</i>	11
2.4 <i>Considering Technological Affordances of Mediated Privacy</i>	14
2.5 <i>Privacy in Association with Contemporary Surveillance</i>	19
2.6 <i>Privacy in Association with Misled Media Usage and Moot Modalities</i>	21
CHAPTER 3. METHODS.....	27
3.1 <i>Overview</i>	27
3.2 <i>Participants</i>	27
3.3 <i>Procedures</i>	30
3.3.1 <i>Stimuli Design and Categorization</i>	30
3.3.2 <i>Study Procedure Overview</i>	32
3.4 <i>Measurement</i>	33
3.4.1 <i>Measured IV: Awareness of Mediated Privacy</i>	34
3.4.2 <i>Measured DV: Awareness of Affordances</i>	34
3.4.3 <i>Measured DV: Awareness of Surveillance</i>	35
3.4.4 <i>Measured DV: Usability</i>	36
3.4.5 <i>Data Analysis Strategy</i>	37
CHAPTER 4. RESULTS.....	40
4.1 <i>H₁, RQ₁, H₂</i>	40
4.2 <i>RQ₂</i>	41
4.3 <i>Additional Analyses: Qualitative Content Analysis</i>	42
4.4 <i>Synopsis</i>	44
CHAPTER 5. DISCUSSION	47
5.1 <i>Overview and Explanation of Hypotheses/Research Questions</i>	48
5.1.1 <i>H₁, RQ₁: Privacy Awareness and Awareness of Affordances</i>	48
5.1.2 <i>H₂: Privacy Awareness and Awareness of Surveillance</i>	52
5.1.3 <i>RQ₂: Privacy Policy Modality and Privacy Decisions</i>	53
5.2 <i>Implications of Findings and Future Directions</i>	57

5.2.1	Theoretical Implication: Toward a contemporary conceptualization, and theory, of privacy. 58	
5.2.2	Theoretical Implication: Reconsidering privacy from an affordance perspective.	59
5.2.3	Theoretical Implication: Reconsidering privacy within the contexts of DoI and MAIN.....	62
5.2.4	Practical Implication: Much ado about privacy policies.....	63
5.2.5	Theoretical & Practical Implications: Encryption, end users, and you.....	64
5.3	<i>Limitations and Future Research</i>	65
5.4	<i>Summary and Conclusion</i>	67
APPENDICES.....		69
APPENDIX 1. STUDY MEASURES.....		69
APPENDIX 2 Stimuli Used (Privacy Policies).....		75
REFERENCES.....		95
VITA		111

LIST OF TABLES

Table 3.1 Descriptive Statistics for Study Variables	39
Table 3.2 Frequencies of Consent.....	39
Table 4.1 Descriptions of Themes	45

CHAPTER 1. INTRODUCTION

1.1 The Problem of Privacy

Congratulations! If you are reading this document, then you have, at some point, given away your privacy. You most certainly have done so when you browsed the Internet on May 25, 2018, and were presented with a new privacy policy and/or terms of service (ToS) agreement on every single website you visited because of the implementation and enforcement of the European Union's General Data Protection Regulation (Jeong, 2018). Were the terms of service too long or confusing? Did you want to dismiss the notification that popped up on the screen? Did you just not care enough? Did you want access to your brand-new iPhone? Regardless of the reason, checking the "I Agree" button gave away your privacy and holds significant implications for you as a user. Furthermore, you are probably not the only person who has done this.

Every day, millions of young adults use their devices to log onto seemingly innocuous social media platforms that collect large amounts of data from these users (e.g., Facebook, TikTok; Fowler, 2020). These same individuals are also eager to adopt new technologies (e.g., Amazon Alexa) that store individuals' voices, home addresses, and other personal details while also containing significant security flaws (Doffman, 2020b). When these users are asked about their online privacy, they claim to be both knowledgeable and concerned about their data. Yet, they fail to take any initiatives to protect themselves. The general concern that people express in the face of known online privacy risks is known as the as the privacy paradox (Barnes, 2006). Knowing that the average user is the weakest link in the cybersecurity chain (Culp, 2016), it is possible that communication theory could explain and/or hypothesize behaviors associated with the privacy paradox. Unfortunately, this is not the case. Communication theory lacks a cohesive explanation for the privacy paradox with regard to how privacy is practiced in the status quo as well as the extent to which one gives their privacy away. Is this paradox a problem of our environment, culture, or something else? Data being given away freely in the status quo and this

is largely due to how users and adopters of technology mismanage their privacy. Thus, the time is now for scholars to reconsider what kinds of variables, be it technological or behavioral, could be related to one's willingness to give their privacy away.

The privacy paradox and related privacy mismanagement behaviors are indeed a problem that communication scholarship may be uniquely positioned to explore. New technologies are introduced and adopted on massive scales, specifically those that are data-driven and request a significant amount of data from their users. An opportunity exists to reconsider the problem of privacy from a perspective that considers both individual differences of technology users and affordances embedded in the technologies themselves.

The present study makes note of the shortcomings of communication theory and proposes the notion of mediated privacy, an understated concept in the field, which functions as an extension of hallmark privacy theories (e.g., Altman, 1975, 1977) as well as Petronio's (2002) communication privacy management. In this vein, the current research elevates the concept of privacy as one being a cultural concept, involving technological and communicative affordances, as well as associated with contemporary surveillance. By elevating privacy in this fashion, it may be possible to explain and address the privacy paradox. The present study avoids contributing to discourse involving the life/death of privacy. Instead, this study shifts the goalposts away from attempting to predict privacy protection in the status quo and is centered in a reality where individuals have haphazardly given their data away and assumes that they will continue to do so. The present study seeks to understand the specific extent one gives their data privacy away to access a new technology by focusing on technological affordances, awareness of privacy, and modalities of privacy policies.

The novel Coronavirus (COVID-19; Feibus, 2020) and the implementation of surveillance applications on college campuses (e.g., SpotterEDU; Harwell, 2019; Schwarz, 2020) indicate that new media technologies and contemporary social issues hold the potential to start conversations regarding privacy. Given the exigence of these issues in tandem with the privacy

paradox, the present study asks college students to report on their privacy habits and awareness to better understand the extent privacy is given away.

CHAPTER 2. LITERATURE REVIEW, HYPOTHESES, AND RESEARCH QUESTIONS

2.1 Overview

In a time where privacy is valued as being worthy of concern, yet knowingly and willingly given away, answering questions related to the extent to which someone gives their privacy away is marred by misconceptions and outdated suppositions related to what privacy *is* as well as assumptions regarding how privacy functions in the status quo. Knowing this is an exigent issue within the literature as well as contemporary human behavior, the purpose of this dissertation is twofold. First, this dissertation seeks to decenter privacy away from its offline roots of being a human-centric unit of study and into a territory where privacy is information-centric and in a constant state of being given away. Second, this dissertation seeks to understand how technological affordances of the privacy consent process and individual difference variables might be related to one another and be catalysts for people keeping (and *knowingly* giving away) their privacy. This should lead to a better understanding of the conditions that surround decisions related to privacy decisions and a better understanding of privacy in general. Ultimately, this dissertation offers insight into the extent to which users might give away their privacy when offered a chance to use a new technology (a practice that has become rather common in today's society).

2.2 On Defining (and Theorizing) a Theory of Privacy

The concept of privacy is rooted in a premise involving offline communication interactions, human stakeholders, and an equal distribution of power between these stakeholders. Multiple scholars have argued that the concept of privacy is a human process (Altman, 1975, 1977), a communication tactic (Petronio, 2002), and a human right (Papacharissi, 2010; Sayre & Dahling, 2016; Warren & Brandeis, 1890). These conceptualizations are important in that they contain the necessary theoretical framework for discussing offline interactions, yet they fall short

in framing contemporary communication phenomena involving privacy practices. Before I can explain this criticism, it is imperative to review these theories of privacy and their conceptualizations.

Some of the earlier conceptualizations of privacy define it as a communicative act that lacks intent, structure, and direction. Westin (1967) defines 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). This description is framed around an individual limiting themselves from being accessed by others but does not explicitly link this act as one being driven by an intent to be secretive. Altman’s (1975, 1977) definition, like Westin’s, lacks an intent yet still describes a human behavior of selectively controlling an *other’s* access to the self. If one is to frame privacy using either of these two definitions, they would have to exclude an element of communicative strategy when discussing what is, and could be, private.

Privacy has also been defined as a human right. Legal interpretations of privacy frame it as a right to be left alone (see Warren & Brandeis, 1890). In contemporary research, framing privacy as a human right has informed public policy on information regulation (Such & Rovatsos, 2016; Youn et al., 2014) and data collection (Malala, 2016; Shilton, 2009). However, like the theories of privacy from Altman and Westin, privacy as a human right is often overlooked in favor of privacy within interpersonal communication settings, such as Petronio’s (2002) communication privacy management.

Petronio’s (2002, 2013) communication privacy management (CPM) is a hallmark theory used to guide privacy in an interpersonal setting. In that vein, privacy in interpersonal settings is a communication tactic, involving a process of constructing boundaries, revealing information, as well as the extent to which those boundaries are managed by information stakeholders. Privacy, then, is “the feeling that one has the right to own privacy information, either personally or collectively” (Petronio, 2002, p. 6). Research using this conceptualization has involved understanding the boundaries of friendships (Kennedy-Lightsey et al., 2012), infertility

disclosures (Steuber & Solomon, 2012), e-commerce (Metzger, 2007), and a willingness to allow increased government surveillance (Rulffes, 2017). CPM has also been used to guide research on social media users and their (lack of) privacy online, such as the kinds of content individuals are willing to share with others on their social media feeds (Ampong et al., 2018; Child et al., 2012; Choi & Bazarova, 2015; Ellison et al., 2011; Quinn, 2016), how identities are managed through using social media (Livingstone, 2008), as well as awareness of privacy in online settings (David & James, 2013; Shreeves, 2015). At its core, CPM is valuable for communication research because it details the human communication processes related to practicing privacy, how information *should be* shared between human actors, as well as how privacy influences interpersonal communication concepts (e.g., maintaining relationships). However, there are multiple limitations (i.e., assumptions) regarding interpreting privacy solely as a human right, a communication tactic, and a communication act lacking intent.

First, contemporary privacy theories are imprecise in their powers to explain what privacy is as well as what privacy could be in mediated settings. In other words, these theories fail to account for how privacy is practiced in social media between data owners (i.e., social media users) and data controllers (i.e., social media platforms). The notion of the disproportionate relationship between data controllers and data owners might be missing from communication theory, but it can be contextualized using an example of contemporary data sharing. Consider an agreement that a social media user reviews before being given permission to access the platform. The user is presented with a lengthy privacy policy with a checkbox that indicates their understanding *of* and agreement *with* this policy. While this scenario is technically one that is not compliant with the *General Data Protection Regulation (GDPR)*; for a review of the *GDPR*, see General Data Protection Regulation [GDPR], 2016), it is a scenario that contrasts with Petronio's (2002) second and third suppositions of CPM involving the creating and maintaining of privacy boundaries as well as controlling and owning private information.

The second supposition of CPM states that, while privacy boundaries can be differentiated depending on who is involved as well as the type of information being regulated (i.e., shared), the ambiguous *or* clear lines of ownership are usually dependent on *who is responsible for the information being shared* (Petronio, 2002). For the case of the aforementioned example, this would mean that the user would still be responsible for their data long after enacting the privacy policy. This is not the case in the status quo as the data owner becomes responsible for that data being held secure. Furthermore, the data owner's presentation of the privacy policy determines which information is private and public information that could be at odds with the user's presupposed idea of what is and should be private. Although CPM lightly accounts for this discrepancy in the form of boundaries shifting over time as one ages, it does not account for the *decrease* of a privacy boundary because of a nonhuman entity's (i.e., a data controller's) influence over determining what is considered to be private data.

The third supposition of CPM states that due to an individual need to exercise and maintain control, one manages that control through the regulation of the boundaries described in the second supposition. In other words, when one shares information with another, both parties become mutual co-owners of that private information, both with different sets of responsibilities involving that private information (Petronio, 2002). For the case of the aforementioned example involving the data owner and data controller, the relationship between the two would involve a mutual creation of privacy boundaries, protection of, and a stake in the mutual maintenance of that information remaining private. However, this does not occur in the status quo because of an imbalance of power that exists between data controllers and data owners. Data controllers such as Facebook *create* the boundaries for *future information* that they will co-own; the users who partake in that privacy policy have no choice in modifying that policy (MacKinnon, 2012). Either the user agrees to *all* of the privacy boundaries set by the data controller who does not co-own the information *yet*, or they are not allowed to access the platform. This problematic dichotomy holds the user hostage in their decision-making; research should be concerned with how this might

impact our considerations of privacy going forward. Although human communication research has little concerned itself with legal scenarios involving terms of service between human and nonhuman entities, it *should* given how privacy is created, maintained, and enforced within the status quo.

The second shortcoming of privacy theories is their inability to account for contemporary privacy problems: the *privacy paradox* and the *personalization paradox*. These two paradoxes have manifested themselves into problematic influences on mediated human behavior.

The privacy paradox is the end-result of lax users who have become the weakest link of an online security chain connecting concerned citizens to their data. It can best be described as a disconnection between users' privacy attitudes and their resultant online behaviors (Barnes, 2006; Quinn, 2016). Specifically, the paradox can occur when social media users who have checked the box of an overly complicated and verbose privacy policy report concerns with their online privacy while simultaneously handing over their data to a social media platform just to get access. While this could be argued to be an extension of users fearing government surveillance and omnipresent data collection (6 et al., 1998), this issue is exigent because of how it is a risk involving social media use, data security, and the protection of users' rights (i.e., their right to privacy).

Like the behavioral contradictions found in the privacy paradox, the personalization paradox also involves privacy attitudes and behaviors in mediated settings. It can best be described as the contradiction occurring when individuals report their concerns with advertisers and their resultant advertisements knowing *too much* while also reporting a desire for targeted advertisements that suit their interests (Aguirre et al., 2015). Although the fields of marketing, persuasion, and commerce are most concerned with this paradox because of its association with profit and user engagement (Bragg et al., 2019; Crano et al., 2017; Grier & Kumanyika, 2010; Johnson, 2013, Kim et al., 2019; Kox et al., 2017), it is worth referencing given its association with the privacy paradox. While this paradox is less exigent in that it frames users as those

wanting their privacy invaded for an ideally unique service, it still highlights a clear, common, and present privacy violation that has invaded present-day society.

The existence of these paradoxes in the status quo threaten the applicability of CPM as a theory capable of explaining and predicting a contemporary exigent issue such as the privacy paradox (and to a lesser extent, the personalization paradox). Through the lens of CPM, an individual constructs their own privacy rules and boundaries, allowing for greater control over how third parties might have access to that data, as well as how they experience privacy turbulence when a co-owner mismanages the private information (Petronio, 2002, 2013). A data breach is an example of contemporary privacy turbulence between a data controller (e.g., Internet service provider [ISP], social media company) and a data owner resulting from the privacy paradox. Under CPM, when a data breach occurs, the data owner would expect the data controller to explain themselves regarding why the breach occurred as well as a clear explanation regarding what kind of non-authorized third party had access to that private information. However, neither occur in the status quo. Data owners have few opportunities to determine which third parties see their data after they share it with a data controller, nor do data controllers have an obligation to go beyond the bare minimum to discuss the specific impacts of that data breach (Mayeda, 2016; Zajko, 2018). Thus, CPM cannot explain the lack of control users have over their own data as well as the dis-proportionate relationship between contemporary co-owners of private information (i.e., data owners and data controllers).

The two aforementioned examples (i.e., the irresponsible social media user clicking *I Agree* without reading through a privacy policy and data breaches) are too common in the status quo. Yet, existing communication theory lacks an ability to address these contemporary issues. This does not mean that CPM nor any other pre-existing privacy theory should be used to explain human communication. Rather, these theories are invaluable because of their power in describing human-centered and (mainly) offline privacy practices (Margulis, 1977, 2003; Petronio, 2013).

This also does not mean that privacy research should be atheoretical. Instead, the time is now to approach understanding privacy from the extent to which we give it away.

What *should* the definition and theory of privacy be, then? Given the shortcomings of previous conceptualizations of privacy, as well as the limitations of its existent theories, it is imperative to decenter the concept away from being a human-centric concept and instead treat it as an information-centric concept that exists in both physical and mediated spaces. Having an understanding of what privacy *is* provides us with a greater understanding of how it functions in the status quo. Revisiting the problem of privacy would elevate its uniqueness out of a territory where similar terms dilute its meaning and contribute toward further confusion associated with the contested concept that is privacy (Margulis, 1977, 2003). While the purpose of this dissertation is not to redefine privacy through revisiting theoretical tenets associated with privacy-related behaviors, a definition that accounts for problematic privacy practices is necessary for understanding the foundations of the present study. Thus, I define privacy as a *mediated and intentional state of being where one has the right to conceal information so long as they remain in control of said information*. A *good* theory of privacy, then, would be one that is parsimonious (Littlejohn, 2009), precise (Craig, 1996; Sandelands, 1990), synthesizable (Feyerabend, 1983), and capable of being practiced (Craig, 1999). Finally, a good theory of privacy would keep in mind the recommendations of prior scholars who have studied contemporary privacy.

Knowing the concept of privacy as a mediated concept (i.e., *mediated privacy*) and the qualities of a “good” privacy theory, it is imperative to use these as a foundation for future privacy research. Furthermore, it is also imperative to consider the recommendations made by privacy scholars to advance the study of privacy to be as contemporary as those who practice it as well as be relevant with what is considered to be *privacy* in the societal structures that bind us together (i.e., policies). Thus, privacy should be embedded within an alternative context, reconsidered in terms of the affordances associated with the concept, as well as associated as an extension of contemporary surveillance and problematic media use behaviors.

2.3 Privacy in Alternative Settings

Much of what we know about *interpersonal privacy* is at the individual and community level. We are able to answer questions about micro- and mezzo-level variables relating to privacy in online settings, namely on social media. To maintain their online privacy, users make conscious decisions regarding what to share and withhold from others on their individual social media profiles (Ampong et al., 2018; Child et al., 2012; Choi & Bazarova, 2015; Ellison et al., 2011; Quinn, 2016). These decisions can be made at the content level (e.g., the types of pictures to share on Instagram) and the network level (e.g., who to follow on social media). These same users also use social media to strategically withhold their identities (Livingstone, 2008) and are also generally cognizant of the concept of privacy in online settings (David & James, 2013; Shreeves, 2015). Although this research is grounded in interpersonal communication research processes relating to practicing privacy, it lacks a greater explanation beyond describing these privacy practices.

At the mezzo-level, privacy research has highlighted how users construct their networks while keeping privacy in mind. From this, we have an understanding regarding common trends within specific demographics of users and their online friends as well as the processes related to how and when an offline friend becomes an online friend (Child & Westermann, 2013; Yang, 2018; Yuan et al., 2013). This, too, describes the user as one who places considerable thought into how their online networks are constructed in the short- and long-term, although making a decision to give up one's privacy in favor of an innovation is one that is made in the heat of the moment (see Sundar et al., 2013). Maintaining privacy is often a justification for how users construct their social networks, but not to the extent of ensuring that they are consistently practicing privacy in a way that keeps it. For example, Yuan and colleagues (2013) discuss how privacy (as both an interpersonal process as well as a form of political participation) on Chinese social media has influenced norms and discussions regarding state surveillance and commercial interests (i.e., data collection). Yet, these authors all but discuss how these privacy concerns were

brought to the platform. In other words, how was a concern for maintaining and practicing privacy instilled in these users prior to using Chinese social media? The easy answer to that question is that it was outside of the scope of the authors' study, but it is still worth answering for a greater understanding of mediated privacy.

While knowledge of micro- and mezzo-level variables describe a user's online behavior in relation to privacy, it does not translate to predicting future behaviors involving protecting privacy nor elaborating on root causes of impractical and irresponsible privacy maintenance. In an op-ed on privacy research, boyd (2012) suggested that "we need to let go of our cultural fetishization with the individual as the unit of analysis" (p. 350) by expanding privacy research to be comprised of models, networks, and communities as the research subjects. While this is a promising suggestion, the author lacks an explanation regarding what that looks like, as well as how one is to operationalize this newer line of research. Knowing that privacy research has focused extensively on multiple, yet outdated, levels, one such operationalization could be to reconsider what we associate to be private when we use technology in an attempt to pivot to a focus on micro-level variables in other theoretical contexts.

A reconsidered approach to privacy would be one where we consider privacy as a derivative of a culture of complacency resulting from an overestimation and misuse of affordances, or variables that are derived from long-term behaviors and/or impact a significantly large number of users. Although common present-day mediated privacy issues were less prevalent (if not absent from societal discourse) prior to 2000, 6 (1998) predicted privacy risks (i.e., *slow killers* and *avocational thrills*) that ended up being commonplace in 2020, such as injustices, violations, and biases related to financial data collection (e.g., credit card companies and their decision making processes related to spending habits and/or socioeconomics; Crosman, 2020), the lack of personal control over the collection of personal information (e.g., Facebook's data collection and their resultant data breaches; Badshah, 2018), and privacy risks to dignity in the form of being a public social media figure (e.g., social media influencer; Wakefield, 2019). In

this vein, the privacy risks predicted by 6 (1998) have impacted millions of individuals for a long period of time. Seeing that these risks are prevalent and unlikely to go away soon, it can be assumed that the ways in which we practice privacy (knowing some, if not all, of these risks) are derivative of our contemporary culture.

While interpersonal and other social scientific privacy research has not explicitly linked an individual's upbringing to privacy awareness and practices, there are few notable exceptions which support this notion. First, Shin and colleagues (2012) found that tweens who circumvented their parents' Internet safeguarding measures likely overestimated their online invulnerability and were more likely to engage in risky online behaviors. If this is the case for newer (and younger) Internet users, then an argument can be made regarding newer generations creating and perpetuating privacy-related risks that they eventually take into adulthood. Second, Cheung and colleagues (2016) found that early adopters of cutting-edge health technologies (i.e., health applications, genome sequencing, and wearable health devices) were willing to give their data away to support scientific advancements yet were concerned about the potential privacy risks (thus reinforcing the notion of the privacy paradox in health settings). If this is the case for users who adopt technology at a later time (e.g., laggards), then an argument can be made regarding the omnipresence of the privacy paradox in that it transcends traditional demographics (e.g., gender, age, socioeconomic status) and instead impacts *all* users of new technologies and new information-centric media (albeit, at varying stages depending on when one adopts a technology). Users seem to really want the potential affordances of a new technology (even if it comes at the cost of one's privacy being invaded). Third, Sarabdeen and Moonesar (2017) found that although there is no overarching e-health data privacy law in the UAE, citizens of Dubai reported a high level of trust in their health care providers' data-keeping and privacy practices. If this is the case for other regions of the world with inconsistent (or outright absent) federal privacy legislation (e.g., the United States), then an argument can be made regarding individuals expecting *data*

controllers to protect the privacy of their data subjects. In other words, this culture of compliance might be a result of one thinking that it is not their job to protect their own data.

A reconsideration of the problem of privacy portrays it as one of many scenarios, (1) privacy is an issue related to time and scale (e.g., younger generations adopting lax privacy practices and perpetuating them into adulthood), (2) privacy is an issue related to regional practices and societal expectations (e.g., individuals knowing of specific individuals whose duty is to protect privacy in a region where no such legal expectations exist) and/or (3) privacy is an issue related to technological adoption (e.g., when one adopts a new technology, they will be aware of the privacy risks but will prioritize the affordances of that new technology). If any of these scenarios are true, then it can be assumed that ingrained behavioral values drive one to be lax with their own privacy practices. Regardless of which of these scenarios hold water, users are cognizant of their own mediated privacy yet fail to employ tactics to actually protect their privacy. This is but one possible explanation for a lax user at protecting their own privacy; perhaps an alternative explanation exists from the lens of an affordance perspective.

2.4 Considering Technological Affordances of Mediated Privacy

An affordance perspective might yield a clearer understanding of privacy in mediated spaces. Gibson (1986) defined an affordance as “what it [an environment] offers an animal, what it proves or furnishes” (p. 127). In more specific terms, affordances are human perceptions (i.e., their awareness) of an object’s utility drawn from environmental cues. A communicative affordance, then, is “an interaction between subjective perceptions of utility and objective qualities of the technology that alter communicative practices or habits” (Schrock, 2015, p. 1232). As noted by Nye and Silverman (2012), affordances can also be considered dyadic relationships between an agent and an object and include a body of study measuring awareness, simulation, adaptation, and cognition. For the case of this study, one’s awareness of privacy is a key variable.

Communication research involving affordances has evolved beyond classifications and typologies. Communication affordance literature includes, but is not limited to analyzing

behaviors impacted by ICTs (Areepattamannil & Khine, 2017; Rice et al., 2017) granular social media use (Aladwani, 2017; Bowman et al., 2012; Miller et al., 2019), classifying media users (Brandtzaeg, 2010; Karahanna et al., 2018), as well as discussing the communication discipline (Vorderer, 2016). This research has demonstrated that the affordance perspective offers a wide breadth of use cases for analyzing various communication phenomena. Including privacy in this line of research would give privacy researchers the opportunity to decenter the concept of privacy away from being a human-centric issue into an information-centric issue as well as understanding how privacy is considered by media users (if at all) during an age where a great deal of human behavior is mediated and involving non-human actors. Although privacy itself cannot *be* an affordance (as privacy is an *outcome*; see Evans et al., 2017), an affordance perspective can benefit privacy research given privacy being impacted by new media.

There is ample justification for a communicative affordance approach to studying human communication concepts that have been impacted by new media (e.g., privacy). This approach can highlight a relationship between individuals and technologies (Schrock, 2015), shift a conceptualization away from a technological classification schema to broader understanding of higher order behaviors (Faraj & Azad, 2013), and offer historical comparisons between differing technological forms and seemingly novel technological features (a common issue when studying emergent new media; Woodruff & Aoki, 2004). Thus, for the case of privacy, a communicative affordance perspective would yield an understanding of how (and if) privacy is considered when using new media.

Research involving social media affordances and perceptions of that media has given us insight into *why* one might use a particular social media platform over another. However, a common theme in this line of research is that privacy is an implicit variable (assuming it is mentioned at all). Miller and colleagues (2019) found that a tension exists between Twitter users' needs to build an audience, document information, and sending/receiving information. The authors discussed how the platform has changed what people think is acceptable to speak up

about regarding information freedom. In this case, privacy is an implicit/assumed variable in that Twitter users want to build an audience (thus decreasing privacy) but also want to regulate the kinds of information they share (thus maintaining their privacy). The authors all but describe this as an example of the privacy paradox, where one wants to freely share information as a means of building an audience of peers but also is expected to be concerned about the kinds of information they share. Areepattamannil and Khine (2017) found that social media use correlates to enjoyment, recreation, and self-concept. While this study lacked an explicit link to privacy, the authors note that adolescent use of ICTs for recreation leads to greater frequency of use altogether (which in turn could lead to other behavioral variables).

Scholars focusing on social media use have identified several communicative and technological affordances that can be linked to privacy risks outlined by 6 (1998). Social media use affordances include, but are not limited to, varied visibility (Siegert & Löwstedt, 2019) and/or anonymity (Evans et al., 2017; Fox & Potocki, 2014), end-to-end encryption (Doffman, 2020a; Hesse, 2020; Santos & Faure, 2018), and agency (Rathnayake & Winter, 2018; cf. Sundar [2008]; cf. Sundar & Limperos [2013]). While it can be assumed that privacy is related to these affordances in that managing one's online presence by using available technological affordances can allow them to be private, both of these affordances contribute to the risk of *avocational thrill* discussed by 6 (1998). When one chooses to spotlight themselves by amassing an audience and making themselves publicly identifiable, they run the risk of having their privacy violated because of how they willingly gave others the opportunity to violate their privacy. However, there is little discussion of this, along with other privacy risks, within affordance literature; it is imperative for a discussion on how specific affordances can be linked to privacy risks.

Visibility is one such technological affordance with roots in privacy management behaviors and implicitly related to privacy risks. As noted by Evans and colleagues (2017), visibility is an affordance that expands beyond one's ability to display themselves and is instead concerned with how one can control the visibility of their *information* (i.e., data) to another user.

Varied visibility on social media can involve one's ability to selectively display their availability (i.e., mediated presence) to be seen as online and offline (see Siegert & Löwstedt, 2019).

Visibility is implicitly related to privacy risks in that users *could* selectively share very little data with others because they want a decreased online presence, but they could also do so because of how visibility is integrated within that technology. For example, it is not required nor innovative for one to geo-tag a photo on Instagram or Snapchat, but the feature is available for those who choose to do so. Thus, it is imperative to gauge the relationship between the affordance of visibility and one's privacy concerns.

Persistence is another technological affordance with roots in privacy management behaviors and implicitly related to privacy risks. This affordance has been linked to archivability (Ellison et al., 2015) and durability (Treem & Leonardi, 2012) in the sense that an online presence and/or set of information has the capabilities of retaining its presence for others to see as well as its integrity for others to interpret. Like visibility, persistence is not an outcome nor feature of using social media or new technologies, but instead varies across platforms and mediums (Evans et al., 2017). For the case of privacy, it can be assumed that lesser persistence in the form of a self-destructing message (i.e., a Snap on Snapchat) could be considered a more private form of communication, but that persistence might not be the justification for why one uses the feature/platform to begin with. Thus, it is imperative to gauge the relationship between the affordance of persistence and one's privacy concerns.

Although a common trend in social media affordance literature is a lack of explicit privacy discourse, there are few exceptions. One such exception discusses a facet of privacy when using the platform. Santos and Faure's (2018) analysis of *WhatsApp*, a messaging service now owned by Facebook, was highly descriptive in discussing the technological affordances of the service. The authors compared how WhatsApp implemented and discussed specific technological features (including those that preserved privacy; i.e., end-to-end encryption) in comparison to WhatsApp's competitors. The authors found that privacy-focused messaging platforms,

WhatsApp included, self-advertise as being privacy-focused yet implement varying degrees of privacy-keeping affordances. For the specific case of WhatsApp, the implementation of end-to-end encryption maintains a level of privacy by preventing third parties from accessing messages sent on the platform but fails to prevent WhatsApp users from leaking the messages themselves (thus contributing to boundary turbulence). While this finding is valuable in that it highlights a clear weakness in the supposed privacy-protecting nature of that platform, it all but describes if, and how, users seek that platform *for the purpose of privacy*. In other words, how do certain affordances factor into one deciding to use WhatsApp over another service, such as Telegram?

Another exception to the trend of privacy being absent from social media affordance literature involves a reiteration of common trends found in privacy literature, specifically the focus on interpersonal affordances adjacent to privacy. Siegert and Löwstedt's (2019) study on online boundary works sought to understand how social media use influenced the work-life balance of government employees. While this study focused on online interpersonal affordances (i.e., varying degrees of visibility in online spaces and having a persistent online presence), some of their results included *interpersonal privacy risks* (e.g., fearing offline retaliation resulting from an online faux pax). The shortcoming with this is twofold. First, it does not *explicitly* explain the role privacy plays when one behaves online. Second, it does not *explicitly* discuss privacy behaviors that are *exclusive to online settings*. Knowing these shortcomings are not exclusive to affordance literature is an indication that there is room for a study *focusing on mediated online behaviors and privacy awareness*.

A study seeking to understand privacy awareness and specific behaviors online should look to prior studies on affordances involving social media use. We know that privacy is considered when behaving online, but keeping in mind specific affordances unique to social media might give us a greater understanding of which online affordances are closely related to one practicing privacy. Technological affordances that *specifically* invade one's own privacy (e.g., geotagging a photograph on a social media) might give us greater insight as to how one

considers privacy when using social media. Furthermore, the complacency associated with the privacy paradox, as well as the apparent apathy and cynicism associated with taking the steps to *proactively* preserve privacy might indicate a negative relationship between using the available technological affordances to preserve privacy and privacy awareness (Hargittai & Marwick, 2016). Knowing the trend of privacy-adjacent concepts and the benefits of the communicative affordance perspective, the present study seeks to answer the first research question and first hypothesis of:

RQ₁: What kinds of technological affordances are associated with greater awareness of privacy?

H₁: Awareness of mediated privacy is correlated negatively with awareness of privacy affordances.

2.5 Privacy in Association with Contemporary Surveillance

Surveillance, or “the systematic monitoring of people or groups in order to regulate or govern their behavior” (Monahan, 2011, p. 498), is a concept worth discussing in relation to contemporary privacy. While privacy literature is not explicit with associating awareness of surveillance and the tangible effects of being watched, much of surveillance literature links to privacy issues. Modern technological advances and contemporary risks have caused us to assume that all of our verbal and nonverbal behaviors are being monitored in airports (for national security purposes; Adey, 2006) and in the workplace (Kizza & Ssanyu, 2005). We know that our Internet histories as well as the devices we own are subject to being used by our government for monitoring us and those around us (see Caluya, 2010). There is also a risk of us showing up on someone else’s social media feed or an amateur recording (Koskela, 2004, 2009). It is very easy to assume that privacy is dead because of the magnitude of surveillance occurring in the status quo (Lyon, 2010). However, the concerns of being surveilled (be it from an intentional government actor or on social media) are similar to the privacy risks outlined by 6 (1998); the *slow killers* and *avocational thrills* can be associated with surveillance issues. There could be

long-term effects of being monitored (i.e., an effect of a *slow killer*) as well as shown on someone else's social media feed (i.e., a side effect of our willingness to use social media via an *avocational thrill*).

Surveillance's embeddedness within our culture seems to mirror the problem of the privacy paradox. Monahan (2011) argues that a reflexive approach for understanding this embeddedness is necessary for a cohesive understanding of contemporary surveillance. While the author does not make explicit recommendations for how this reflexivity can be operationalized (see also boyd, 2012), one such way of enacting that reflexivity can be through understanding how awareness of surveillance is related to awareness of privacy, if at all.

Research on surveillance awareness has been generally descriptive for understanding how our behaviors change once we learn we are being watched. Workplaces who enact "performance monitoring" ICTs (e.g., web filters) to deter workplace loafing cause resentment among employees (Lim, 2002) as well as create a workplace atmosphere of fear and mistrust (Kizza & Ssanyu, 2005; Mujtaba, 2003). In instances where employees are already aware of pre-existing acts of surveillance, the introduction of new measures (i.e., an organization decides to implement a new monitoring technology) causes workers to harbor negative feelings toward their employers (Martin et al., 2016; Sarpong & Rees, 2014). Thus, *knowing* that someone is *now* watching with some form of repercussions changes one's behavior.

There is a key implication of these findings in relation to privacy literature. Our concerns about surveillance might be present, yet are amplified when we are made aware of a new instance of surveillance and/or our expectations regarding surveillance are violated. These concerns function like privacy concerns in that individuals are knowledgeable yet apathetic about their privacy unless or until something tangible happens to them (see Hargittai & Marwick, 2016). If this is the case, then a relationship might exist between awareness of surveillance and privacy. Thus, the study's second hypothesis is:

H₂: Awareness of mediated privacy is correlated positively with awareness of surveillance.

2.6 Privacy in Association with Misled Media Usage and Moot Modalities

Before one can gain access to a social media platform (or a new media technology), they must agree to a privacy policy. A frequent cause of privacy mismanagement exists in the form of skimming through that privacy policy before using a new application. In the present day, privacy policies have been constructed around contemporary privacy legislation, such as the European Union's *GDPR* (GDPR, 2016) and California's *California Consumer Privacy Act (CCPA)* (Sirota, 2019), as a means of protecting the end user from privacy risks. Whether or not these policies protect users' privacy is outside of the scope of this study, but understanding how one (ir)responsibly interacts with a privacy policy might lend insight into addressing the privacy paradox, specifically in relation to the affordances offered by a privacy policy.

The easiest explanation for users' lax behavior is that a user does not have the time nor interest in reading through a convoluted document because of how consent processes have become routinized (Ploug & Holm, 2013). Another easy explanation for this can exist in the form of policies being constructed without requiring users to actually read the policy and instead skip ahead to the "I Agree" button (which is not compliant with the GDPR [GDPR, 2016]). Rossi and Palmirani (2017) argue that because most privacy policies and terms of service (ToS) agreements are dense, unintuitive, and lack plain language, alternative formats of displaying these policies (e.g., images, quizzes) might assist in informing users of what users are giving up (i.e., their privacy) in exchange for access to the application. Although regulations such as the GDPR have taken steps at standardizing how privacy policies are displayed to end users (see Katulić & Katulić, 2018), users still skip past the text and seek out the "I agree" checkbox. While readable and simplified privacy policies might not be standard and available in the status quo, it would seem likely that users would react differently to seeing alternative elements (e.g., pictures) in a

privacy policy compared to a problematic policy oft-found in our daily lives. In short, *modality matters*. A study involving privacy policies displayed in different modalities can yield a greater understanding into how one gives away their privacy in order to access a new technology. While it can be assumed from the literature that individuals might seek out the “I agree” button on a page to skip past a gigantic privacy policy, the literature lacks explanations regarding how one interacts with a policy that has been condensed and/or reformatted for easier understanding. The ways in which one interacts with a privacy policy in a(n) (ir)responsible fashion can be further explained from the lens of mass communication theories, specifically those that pertain to media use.

The paradoxes of personalization and privacy can be explained using the lens of media use theories, such as the diffusion of innovation (DoI) and the MAIN model. Both theories are capable of predicting and describing the extent to which one adopts, uses, and continues to use a new technology. With regard to the paradoxes of privacy and personalization, these theories also offer insight into the extent one *gives away* their privacy in exchange for access to a new technology.

Rogers’ (1962) diffusion of innovation (DoI) has been used in communication research to predict and describe how users apply new technologies (i.e., innovations) to their lives over time. The theory argues that the success of those new technologies depends on how they are introduced, how users discuss those technologies, how those discussions diffuse through other networks, and how quickly those technologies and resultant discussions diffuse through other networks. DoI tends to focus on specific forms of communication and information found on new media (e.g., Twitter; English, 2016; Schwartz & Grimm, 2017). Although privacy might not be found in the communication literature as an outcome variable related to a new technology’s diffusion through society, legal studies literature argues that privacy would *prohibit* the diffusion of new innovations. Bernstein (2006) considers privacy risks a threat to the diffusion of new technologies regardless of the threat’s likelihood. If this was the case in the present day, then

invasive technologies would not be adopted at their current rapid rate. However, the inverse is occurring. Knowing that technologies are becoming increasingly invasive, DoI might not be fit for predicting the success of those technologies. Instead, it can be used as a reference for predicting *how a user* could adopt a technology and the effects of doing so.

Sundar's (2008) MAIN model determines how users perceive credibility from new media. Rather than focusing on the content of the medium, MAIN focuses on technological cues that are tied to judgements, be it cues of modality, agency, interactivity, and/or navigability. Although this theoretical foundation has not explicitly been used with privacy research, specific tenets (i.e., affordances) of the model have been used to determine how one might use a new form of *invasive* technology, namely *agency* and *modality*.

The affordances of agency and modality are associated with how one decides to use a new technology, specifically one that infringes upon one's online privacy. Sundar and Marathe (2010) found that privacy was a key predictor of user attitudes toward personalization and customization of news feeds in that giving users a greater sense of agency caused average users to respond favorably to tailored content (thus confirming the personalization paradox), whereas power users (i.e., those with high technological expertise) need assurances regarding their control of their privacy (thus confirming the privacy paradox). Cho and colleagues (2020) note a similar finding in their study on smart speakers (e.g., Amazon Alexa-powered devices); users who were the most privacy-conscious were most likely to delete their voice recordings (i.e., take the steps to preserve their privacy) yet reported a decreased user experience when presented with the opportunity to customize their privacy using the interface (similar to the cynicism noted by Hargittai & Marwick, 2016; thus confirming the privacy paradox). In sum, when given the option to *do something* about protecting one's own privacy when using a new technology, even the most technologically savvy and privacy-conscious individual begrudgingly took the step to protect themselves.

DoI and the MAIN model support the privacy and personalization paradoxes. With regard to DoI, widespread technological adoption will occur despite a technology's problematic nature in cases where that technology meets a need (i.e., innovates a process) of a significant number of individuals. If a new technology offers an individual a novel way of meeting a communication need in exchange for a massive amount of user information, it can be assumed that it is only a matter of time before others will follow suit and give up their information in the name of customization. With regard to MAIN (or specific affordances therein), widespread technological adoption can occur due to a variety of heuristics (e.g., bandwagon, helper, bells-and-whistles, and novelty; see Sundar, 2008). If an invasive technology contains enough novelty, or enough individuals use it to the point of others being influenced to do so, too, it can be assumed that both the average user and power users will give away their information in exchange for access to that new technology (although power users might begrudgingly or concernedly do so). Because of the inevitable adoption of invasive technologies, it is worth moving past questioning how we can preserve one's privacy post-hoc but instead gauge the extent one would give away their privacy in exchange for technological access.

The present study takes these considerations in mind in that there might be differences in one using a privacy policy when it is presented in a myriad of fashions. Thus, the present study seeks to manipulate several aspects of the privacy policy consideration process for a greater understanding into the environment in which one gives their privacy away. Manipulating the privacy policy's structure (i.e., a full policy, a summarized policy, and a policy containing imagery) might yield an understanding into differences between how one consents to have their privacy given away. Manipulating the content of a privacy policy (i.e., a policy about a health technology and a policy about a clothing application) might yield a clarification regarding how one might *want* to give their privacy away in exchange for a personalized experience.

New technologies and contemporary social issues seemingly unrelated to privacy are bound to involve privacy as they become more feature-filled (or data-driven) and interwoven

between multiple public spheres. Universities across the US are creating and implementing smartphone applications to track students' behaviors in the classroom for the purpose of academic honesty and class attendance (e.g., SpotterEDU; Harwell, 2019; Schwarz, 2020). The novel Coronavirus (i.e., COVID-19) has impacted multiple industries and brought together the fields of health, new technology, and law to prevent the spread of COVID-19 worldwide through the implementation of contact-tracing applications (i.e., applications that track one's GPS location and notify them in the instance when they were in close contact with an individual who has tested positive for COVID-19; Byford, 2020). Although implementing these apps has proved difficult for technological, fiscal, and governmental reasons (Browne, 2020), misinformation campaigns on social media highlighted a significant privacy concern among social media users. That is, people are concerned (some outright unwilling) to use these applications because of how they potentially invade one's privacy through permanently utilizing the GPS on one's smartphone (Dev, 2020; Feibus, 2020). While this concern might be linked to conspiracy theories regarding new technologies, it highlights how a new technology created to aid public health is pushed into a territory involving privacy concerns.

Although contact tracing has been employed (with varying degrees of success) prior to 2020 to address outbreaks worldwide (Bernard et al., 2018), the sudden concern regarding using contact tracing applications and awareness of individual privacy is important for two reasons. First, it supports the notion that, while we might be under constant surveillance under the status quo, we might not concern ourselves with surveillance until a new method of surveillance is suddenly and visibly introduced (Martin et al., 2016; Sarpong & Rees, 2014). Second, and most importantly, it contradicts the notion of how users adopting a cutting edge technology might willingly give up their privacy in order to access an affordance of that new technology, such as a new health technology aiming to benefit public health (Cheung et al., 2016). There seems to be an extent to which one knowingly and willingly gives up their privacy. Thus, the study seeks to answer the final research question of:

RQ₂: How does the modality of a privacy policy factor into individuals making privacy decisions?

CHAPTER 3. METHODS

3.1 Overview

The purpose of this study was to better understand the extent to which, and affordances related to individuals perceiving their privacy when presented with privacy policies, as well as understand the relationship between individuals' reported privacy beliefs and their awareness of online privacy. To answer the study's research questions and hypotheses, the present study employed a 2 (health or personalization) x 3 (full, partial, or picture policy) between-subjects design experiment with a control condition (no treatment). The study involved deception in that students were asked to evaluate a "new app" for smartphones and encouraging them to read through a type of privacy policy/description.

3.2 Participants

The study's participants were obtained via convenience sampling from a population of undergraduate students at a large southern university. After receiving IRB approval, participants were recruited using the university's SONA system (i.e., an online participant recruitment system that offers college credit in college communication courses). To be eligible for the study, participants had to be at least 18-years of age. This population was chosen because of the convenience offered by recruiting available participants as well as the appropriateness of having young adults participate in a study on topics that might concern them (e.g., privacy during a pandemic period). To detect a moderate effect size at the 0.8 level, an *a priori* power analysis was conducted using G*Power 3.1 and determined that a minimum of 222 participants was needed for the present study's 7 total conditions (i.e., ~30 participants per condition). Because the study employed deception, the IRB required the use of a debriefing and opt-out system at the end of the survey that informed participants of the true nature of the study as well as an opportunity to withdraw without penalty. To account for attrition in the form of participations choosing to opt out, at least 250 participants were initially requested.

When data collection had concluded, 284 participants had taken the survey. Several procedures were used to assure sample quality: (1) excessive speed of response, (2) explicit requests to opt out of the study, and (3) gross incompleteness. There were 5 participants omitted for taking less than one minute to complete the survey. The average participant took 9.23 minutes to complete the survey. There were 17 participants who were omitted for explicitly requesting to opt out. There were 6 additional participants who were removed for leaving at least 15 consecutive items blank. Thus, the *final* sample contained 256 total participants ($N = 256$).

In terms of university class standing, the sample featured diverse representation across all cohort years with the exception of graduate/professional students. The sample was made up of a population that consisted of 34.8% ($n = 89$) first year students, 7.0% ($n = 18$) sophomores, 35.9% ($n = 92$) juniors, 21.9% ($n = 56$) seniors, and one (0.9%) graduate/professional student. In terms of gender, participants were mainly female. The sample was made up of 34.0% ($n = 87$) males, 65.6% ($n = 168$) females, and one (0.4%) non-binary/third gendered individual. Participant ages ranged from 18 to 53, with an average age of 20.65 years old ($SD = 4.02$) and median age of 20 years old. Nine participants declined to report their age. Participants were given the opportunity to report their ethnicity or ethnicities, if applicable. The sample was overwhelmingly white/Caucasian. In terms of ethnicity, 80.1% ($n = 205$) identified as white/Caucasian, 11.7% ($n = 30$) identified as black/African American, 7.4% ($n = 19$) identified as Asian/Pacific Islander, 2.0% ($n = 5$) identified as Latino/Hispanic, 1.2% ($n = 3$) identified as American Indian/Alaskan Native, and one individual (0.4%) wrote in their ethnicity. In terms of sexuality, the sample was comprised of almost all heterosexuals. In terms of sexuality, 94.1% ($n = 241$) identified as heterosexual (straight), 0.4% ($n = 1$) identified as gay, 0.4% ($n = 1$) identified as lesbian, 3.1% ($n = 8$) identified as bisexual, 0.8% ($n = 2$) identified as asexual, and 1.2% ($n = 3$) identified as “Other” and wrote in their sexuality as an option not listed on the survey. In terms of political affiliation, respondents were primarily liberal or conservative, with 28.1% ($n = 72$) identifying as liberal, 33.6% ($n = 86$) identifying as conservative, 16.8% ($n = 43$) identifying as independent,

19.1% identifying as unsure, and 2.3% ($n = 6$) identifying as another affiliation unlisted on the survey.

Participants were given the opportunity to report their smartphone usage and social media usage. In terms of the number of apps that participants had installed on their smartphones, 250 participants reported a median number of 33 ($M = 44.63$, $SD = 31.15$) and 6 participants declined to answer. In terms of the type of smartphone participants used, 94.9% ($n = 243$) owned iPhones and 5.1% ($n = 13$) owned Android devices. With regard to social media usage, most participants reported to be frequently checking their social media each day. In terms of frequency of usage, 35% ($n = 92$) reported to check their social media every hour, 44.1% ($n = 113$) reported to check multiple times a day, 12.1% ($n = 31$) reported to check a few times during the day, 4.7% ($n = 12$) reported to check at least once a day, 2.0% ($n = 5$) reported to check a few times a week, 0.8% ($n = 2$) reported to check less than a few times a month, and 0.4% ($n = 1$) declined to answer. The median number of hours per week participants used social media was 12 hours ($M = 17.54$, $SD = 19.80$).

Participants were given an opportunity to list which social media applications, if any, they used on a regular basis. Participants were most likely to use Snapchat and/or Instagram. In terms of which social media applications participants used, 90.2% ($n = 231$) reported to use Instagram, 90.2% ($n = 231$) reported to use Snapchat, 68.8% ($n = 176$) reported to use TikTok, 67.6% ($n = 173$) reported to use Facebook, 59.4% ($n = 152$) reported to use Twitter, 41.0% ($n = 105$) reported to use LinkedIn, 14.5% ($n = 37$) reported to use Reddit, 4.7% ($n = 12$) reported to use tumblr., and 5.5% ($n = 14$) reported to use a social media platform that was not listed on the survey.

3.3 Procedures

3.3.1 Stimuli Design and Categorization

The present study contained six different experimental conditions that varied in terms of the manipulations mentioned above and explained in detail below. The control condition was shown a message saying that the participant was not invited to review an application at this time but would still ask participants to complete the survey. The remainder of the manipulated conditions are broken down by context and modality.

This study required the use of stimuli modeled after smartphone notifications, application (i.e., “app”) store descriptions, and privacy policies that could be seen in the present day and interpreted by members of the general population, more specifically: currently enrolled University students. Considering the recommendations of privacy policy researchers (e.g., Rossi & Palmirani, 2017), two additional privacy policies that corresponded to the conditions intended for this study (i.e., *Partial Policy* and *Picture Policy*) were created featuring condensed and easier-to-understand language as well as images.

Participants were assigned to one of seven conditions (six treatment conditions, one control condition), with the treatment conditions varying by *health* and *personalization and privacy policy modality*. The *Surveillance of Health* condition showed participants a description of a fake COVID-tracing application that is being developed (i.e., *UKCovidWatch*) as well as a mockup of what a “notification” would look like on an iPhone. The app’s description contained a novel COVID-19-tracing application, how it tracked students, and how it worked. This condition was created because of the exigence of COVID-19 as well as the misinformation and public concern related to contact tracing applications (Browne, 2020; Feibus, 2020). This context was also chosen because of its timeliness and exigence related to the COVID-19 pandemic. The *Personalization* condition showed participants a description of a fake application (i.e., *DropWatch*) that notifies users of important sales of products that they may desire (e.g.,

collectible shoes). This condition showed participants a new smartphone application that gives users the opportunity to hand over their personal data (i.e., interests) in exchange for a personalized user experience. This condition was created with the personalization paradox in mind (see Aguirre et al., 2015) as well as prior new media research based on customizing platforms that require information (Sundar et al., 2013; Sundar & Marathe, 2010). Furthermore, an iPhone notification mockup was chosen because of the device's popularity as well as its similarities with other lockscreen notifications.

The other factor, modality, was varied in the following ways: *Full Policy*, *Partial Policy*, and *Picture Policy*. The key difference between these conditions is that the same privacy policy was displayed, albeit with slight differences.

The *Full Policy* condition simply showed participants a large and cumbersome privacy policy (modeled after TikTok's policy) as well as a question at the bottom of the policy asking if they consented to use the application. This modality of privacy policy was selected because of its consistency with other problematic policies that exist in the status quo that are controversially dense, wordy, and lack a means of gauging *informed consent* (Rossi & Palmirani, 2017). For most (if not all) users in the condition, it would be safe to assume that they had encountered a nearly identical policy from another social media platform.

The *Partial Policy* condition showed participants a *summary* of a large privacy policy that is broken down into bullets, as well as a button at the bottom of the policy asking if they consent to use the application and/or a button asking if the participant would like to read the full policy. This modality of privacy policy was selected because of its consistency with policies that are currently compliant with the GDPR (but still problematic).

The *Picture Policy* condition was identical to the *Partial Policy* condition but also featured several images that accompanied the summaries. This modality was selected because of its consistency with the recommendations of prior research involving the implementation of imagery with policies to potentially increase informed consent (see Rossi & Palmirani, 2017).

3.3.2 Study Procedure Overview

Upon beginning the survey, the Qualtrics system randomly assigned participants to one of seven conditions: *Surveillance of Health Full Policy*, *Surveillance of Health Partial Policy*, *Surveillance of Health Picture Policy*, *Personalization Full Policy*, *Personalization Partial Policy*, *Personalization Picture Policy*, or *Control*. Participants were first asked about their social media use (e.g., which social media platforms they use, how they use social media) and demographics (e.g., age, gender, sexuality, class standing). Then, participants were presented with a brief summary of an invasive privacy application (depending on condition). The participants in the *Full Policy* condition were exposed to a gigantic privacy policy modeled after one found on social media (e.g., TikTok). The *Partial Policy* condition participants were exposed to a condensed privacy policy using plain language, short summaries, pages to click through, and a “Click here for more information” button that redirected them to the full privacy policy. The participants in the *Picture Policy* condition were exposed to a condensed privacy policy, too, but featured images alongside the plain language. Participants in the *Control* condition were not be shown an application nor privacy policy at all and immediately proceeded with the rest of the survey that did not involve feedback on the new application.

Participants who were shown an application were asked to give “feedback” on the application using four usability questions. Then, participants were shown 26 items related to their knowledge and awareness of their online privacy. Finally, participants were shown seven items gauging their knowledge and awareness of online surveillance. After the study, participants were debriefed on how the study is not actually about a new smartphone app, but instead a study on privacy awareness. In compliance with the IRB’s requests, participants had the opportunity to withdraw from the study if they choose. After consenting to share their data from this study after being debriefed on the deception, the participants were thanked for their time.

As noted, the Qualtrics system randomly assigned participants to one of seven experimental conditions, albeit at two different stages of the survey. The first random assignment

took place after the participants provided demographic feedback, in which participants were evenly placed into the Health ($n = 83$), Personalization ($n = 84$), and Control ($n = 89$) conditions. Participants in the Health and Personalization conditions were shown different versions of the same application, and then randomly and evenly assigned to the Full Policy ($n = 54$), Partial Policy ($n = 58$), and Picture Policy ($n = 55$).

Thus, the resultant six conditions were Health Full Policy ($n = 27$), Health Partial Policy ($n = 28$), Health Picture Policy ($n = 28$), Personalization Full Policy ($n = 27$), Personalization Partial Policy ($n = 30$), Personalization Picture Policy ($n = 27$), and Control (i.e., No Policy; $n = 89$). Oversampling of the control condition did not occur in that an equal number of participants were placed in the beginning when the initial randomization assigned participants to the control or two treatment conditions. The secondary random yet even distribution that occurred only involved the treatment subconditions and did not require a second control group.

3.4 Measurement

Several items on this study's survey were initially adapted from pre-existing literature on surveillance, privacy affordances, and privacy awareness. Several items from these scales were slightly reworded for clarity for the study's population. Additional scales were created to measure the knowledge of affordance variables. The present study has a measured independent variable (i.e., awareness of mediated privacy), manipulated independent variables (i.e., the experimental conditions), and three dependent variables (i.e., awareness of surveillance, awareness of privacy affordances, and usability). Unless otherwise noted, all items were presented and measured using a 7-point Likert-style of agreement (i.e., strongly disagree, disagree, slightly disagree, neither disagree nor agree, slightly agree, agree, strongly agree).

Mean responses from each statement in the survey measures used in this study were calculated. The items for each dependent and independent measure were used to create scales to test the study's hypotheses and answer the study's research questions. Prior to running analysis, the descriptive statistics for all dependent variables were examined for normality (see Table 3.1).

Means and standard deviations appeared acceptable. For all but two variables, minimum and maximum variables indicated that participants had a variety of perceptions of their online privacy and privacy-adjacent concepts in this study. IBM SPSS 27 was used to check multiple criteria to determine whether the data were suitable for the analysis. The skewness values for all variables were all in the acceptable range of between -1 and 1. The data were checked for outliers using Mahalanobis' distance and were deemed acceptable for univariate analyses.

3.4.1 Measured IV: Awareness of Mediated Privacy

The present study's measured independent variable, awareness of mediated privacy, involved seven items measuring privacy concerns (e.g., *It bothers me when apps ask me to provide personal information*) and five items measuring privacy awareness (e.g., *It is okay for my account provider [such a Facebook] to share my profile information with some websites.*) These were adapted from exigent subscales that have demonstrated significant reliability and used in prior affordance and privacy research (e.g., Adhafferri et al., 2013; Cho et al., 2020; Dinev & Hart, 2005; Koochang, 2017; Krasnova, 2017). These items were intended to measure participants' awareness of their online privacy as it pertained to social media. Although these studies have used multiple subscales to measure awareness and concern of privacy, an exploratory factor analysis (EFA) and scale analysis was run to determine the validity of the Awareness of Mediated Privacy scale. The resultant EFA with varimax rotation indicated a unidimensional factor structure involving 8 (items of the original 12) loading onto a single component; the resultant scale analysis of these 8 items indicated a strong reliability such that a greater value indicated a greater perception (i.e., awareness and concern) of mediated privacy (Cronbach's $\alpha = .93$, $M = 5.29$, $SD = 1.19$).

3.4.2 Measured DV: Awareness of Affordances

The present study's first dependent variable, awareness of affordances, was measured using a novel measure (containing three subscales) created for this study. This measure contained

four items that measured knowledge of Visibility (e.g., *I know how to adjust the visibility of my social media profiles.*), six items that measured knowledge of Persistence (e.g., *I have taken screenshots of my friends' social media posts*), and four items that measured knowledge of Encryption Affordances (e.g., *I have used apps that feature end-to-end encryption*). Items were based on examples of these affordances as described in the literature (e.g., Evans et al., 2017; Miller et al., 2019; Santos & Faure, 2018; Siegert & Löwstedt, 2019). These items were created, rather than adapted from pre-existing scales, because of how these affordances tended to evolve in tandem (often quickly) with their associated technologies. An exploratory factor analysis (EFA) and individual scale analyses were run to determine the validity of the Awareness of Affordances subscales. The resultant EFA with varimax rotation indicated a three-factor structure involving 11 of the 14 items. The resultant scale analyses indicated strong reliability for the Persistence ($n = 3$, Cronbach's $\alpha = .64$, $M = 5.17$, $SD = 1.18$), Visibility ($n = 4$, Cronbach's $\alpha = .67$, $M = 5.70$, $SD = .89$), and Encryption Affordances ($n = 4$, Cronbach's $\alpha = .70$, $M = 4.04$, $SD = .94$) subscales, such that larger values indicate a greater awareness of the aforementioned affordances.

3.4.3 Measured DV: Awareness of Surveillance

The present study's second dependent variable, awareness of surveillance, was measured using seven items adapted from the surveillance scale in Xu et al.'s (2012) information privacy scale (e.g., *I am aware that tagging myself at a location can make my information public*). This specific subscale was chosen because of its reliability in prior research as well as its containing contemporary items of mediated surveillance. Although the scale itself initially created three items, additional novel items were created to enhance the potential robustness for use in this study. The responses to the six items were summed and averaged to create a scale, which was found to be reliable such that a greater value indicated a greater awareness of surveillance (Cronbach's $\alpha = .79$, $M = 5.63$, $SD = .91$).

3.4.4 Measured DV: Usability

Usability was measured after users read through the privacy policies. These four items were created specifically for the study and were used to determine the likelihood of users opting into using the imaginary application. These items asked 1.) if the tool is “effective” at achieving the intended effects (e.g., a typical usability study’s survey items), 2.) if the application met participants’ needs, and 3.) the likelihood of them using it. The usability items concluded with a box for students to write in qualitative feedback. The responses to the four items were summed and averaged to create a scale, which was found to be reliable such that a greater value indicated greater usability (Cronbach’s $\alpha = .85$, $M = 4.11$, $SD = 1.38$). Of the 167 participants who were initially assigned to one of the health and personalization sub-conditions, 39 participants provided qualitative feedback. Of those 39, 31 provided feedback beyond one-word responses (e.g., “N/A,” “none,” “no”).

Usability was also measured by calculating the frequency at which participants consented or not consented to using the application. If participants were placed in the Partial or Picture conditions, they were presented with the option to consent, not consent, or read a version of the full privacy policy. If they chose to read the full privacy policy, they were presented with another consent item. The frequencies of those who consented, not consented, and opted to read more can be found on Table 3.2.

Of the 167 participants who were presented with a privacy policy, 59.3% ($n = 99$) consented, 28.6% ($n = 47$) did not consent, and 12.6% ($n = 21$) opted to read more (involving 6.0% [$n = 10$] consenting after reading more and 6.6% [$n = 11$] not consenting after reading more). Taking policy modality into account, 17.6% ($n = 33$) consented after reading the full privacy policy, 18.1% ($n = 34$) consented after reading the partial policy, and 17.0% ($n = 32$) consented after reading the policy containing pictures. Taking into account the application’s

context (i.e., health or personalization), there were more participants who consented to use the application than not consenting. However, in the picture x health condition, more participants did not consent than those who did consent, whereas those in the picture x personalization condition consented to a far greater extent than those who did not consent. Finally, of the few individuals who opted into reading the full privacy policy, all participants in the picture x health condition did not consent to use the application, whereas all participants in the picture x personalization consented to use the application.

3.4.5 Data Analysis Strategy

In order to answer the aforementioned research questions and hypotheses, the following tests and procedures were outlined and approved. Prior to analysis, scale and exploratory factor analyses needed to be conducted for the novel measures that were created specifically for this study (i.e., Awareness of Affordances). These measures are to be considered reliable if their KMO measures are above the .600 criteria and have a Cronbach's α equal to or greater than 0.7.

The study's hypotheses will be tested by running several correlations between the study's single measured IV (i.e., Awareness of Mediated Privacy) and two DVs (i.e., Awareness of Surveillance, Awareness of Affordances). This will be done because all variables are continuous variables and are not exclusive to the experimental conditions implemented in this study. **RQ1** seeks to understand which kinds of affordances are most associated with awareness of privacy. This will be determined using correlations, too. The affordance submeasure (i.e., Visibility, Persistence, and Encryption) with the greatest correlation to awareness of privacy will answer the research question.

The second research question can be answered by running a 2x3 factorial ANOVA to determine differences between the contextual conditions (i.e., Health and Personalization) as well

as the modality conditions (i.e., Full Policy, Partial Policy, and Picture Policy). This test will be run because the study will have six manipulated conditions, as well as a control. Furthermore, Usability is a continuous measure that seeks to understand how likely one might use a theoretical application depending on its context as well as the modality of its privacy policy. An ANOVA will yield a better understanding of likelihood of future use on a per-group basis.

Table 3.1
Descriptive Statistics for Study Variables

Measured Variable	M	SD	MIN	MAX	Skew	Kurt.	α
Awareness of Mediated Privacy	5.29	1.19	1.00	7.00	-.77	.63	.93
Awareness of Surveillance	5.63	.91	2.67	7.00	-.57	.25	.79
Awareness of Persistence	5.20	1.18	1.33	7.00	-.62	-.10	.64
Awareness of Encryption	4.04	.94	1.75	7.00	.68	.94	.70
Awareness of Visibility	5.70	.89	3.00	7.00	-.51	-.18	.67
Usability	4.11	1.38	1.00	7.00	.08	-.29	.85

Table 3.2
Frequencies of Consent

Condition	Full Policy		Partial Policy		Picture Policy	
	Health	Personalization	Health	Personalization	Health	Personalization
Consent	12	21	16	18	11	21
No Consent	6	15	7	4	13	2
More Information			5	8	4	4
Yes			2	4	0	4
No			3	4	4	0

CHAPTER 4. RESULTS

The present study posed two hypotheses and two research questions the relationship between privacy awareness and related privacy variables (e.g., surveillance), the relationship between privacy awareness and awareness of technological affordances related to privacy, and how individuals react to privacy policies of different modalities.

4.1 H_1 , RQ_1 , H_2

The present study's first hypothesis (H_1) posited that awareness of mediated privacy correlated negatively with awareness of privacy affordances. The study's first research question (RQ_1) sought to understand what kinds of technological affordances were associated with greater awareness of privacy. Several two-tailed Pearson's correlations were conducted between the independent variable of awareness of mediated privacy and dependent variables involving awareness of persistence, visibility, and encryption. With regard to awareness of mediated privacy and awareness of persistence, it was found that no significant relationship existed ($r_{pers} = .05 [-.09, .18]$, $p = .47$). With regard to awareness of mediated privacy and awareness of visibility, it was found that a weak, positive, and significant correlation existed ($r_{vis} = .29 [.16, .41]$, $p < .001$). With regard to awareness of mediated privacy and awareness of encryption, it was found that a weak, positive, and significant relationship existed ($r_{enc} = .35 [.24, .47]$, $p < .001$). Although H_1 is not supported, the technological affordances associated with greater awareness of privacy (that demonstrated significant relationships) were visibility and encryption, thus answering RQ_1 .

The study's second hypothesis (H_2) posited that awareness of mediated privacy correlated positively with awareness of surveillance. A two-tailed Pearson's correlation was conducted between the independent variable of awareness of mediated privacy and dependent variable of awareness of surveillance. The resultant correlation found that a positive and

significant relationship existed between awareness of mediated privacy and awareness of surveillance ($r_{surv} = .54$ [.43, .64], $p < .001$). Thus, H_2 is supported.

4.2 RQ₂

The second research question sought to understand the relationship between the modality of a privacy policy and the variables of awareness of surveillance, intentions to use an invasive application, and awareness of privacy. This research question was answered in the following fashions.

First, a 2x3 factorial ANOVA was conducted between the six experimental conditions and the usability subscale. It was found that there was no significant main effect between being shown a different type of application, modality of privacy policy, and intention to use an invasive application, $F(5, 161) = .514$, $p = .77$, $\eta p^2 = .02$. Individual differences between groups were found to lack significance, as well.

Second, a 2x3x1 factorial ANOVA was conducted between the six experimental conditions, the control condition, and the privacy awareness subscale. It was found that there was no significant main effect between the type of privacy policy displayed, type of application displayed, and awareness of mediated privacy, $F(6, 249) = 1.14$, $p = .34$, $\eta p^2 = .03$. However, there were significant differences indicated in the post hoc tests. Respondents indicated greater awareness of privacy when they were in the control condition ($M = 5.38$, $SE = .13$, $p < .05$) than when they were in the personalization picture policy condition ($M = 4.80$, $SE = .23$, $p < .05$). Respondents also indicated greater awareness of privacy when they were in the health picture policy condition ($M = 5.56$, $SE = .22$, $p < .05$) than when they were in the personalization picture policy condition ($M = 4.80$, $SE = .23$, $p < .05$). There were no other significant differences between any of the conditions in the post hoc tests. Even though the lack of a significant main effect indicates no systematic variability in the outcome, the post hocs indicate specific differences associated with the condition assigned and dependent variable.

Third, a 2x3x1 factorial ANOVA was conducted between the six experimental conditions, the control condition, and the surveillance scale. It was found that there was no significant main effect between the type of privacy policy displayed, type of application displayed, and awareness of surveillance, $F(6, 249) = .93, p = .45, \eta p^2 = .02$. Individual differences between groups were found to lack significance, as well.

4.3 Additional Analyses: Qualitative Content Analysis

Since there were not many experimental main effects found between the modality of a privacy policy shown to participants and their self-reported intentions to use an application, awareness of privacy, and awareness of surveillance, the qualitative feedback was analyzed in order to gain a better understanding of how individuals reacted to these privacy policies. Given that individuals wrote up short statements that reflected more details (in some cases) than their self-reported feedback, it was imperative to run a content analysis to look for trends within the qualitative responses (White & Marsh, 2006).

Qualitative data were analyzed in accordance with mixed method procedures (White & Marsh, 2006) that involve quantitative and qualitative data. For the purpose of this study, the quantitative usability data was a message's tonal valence and qualitative usability data was a message's thematic response. A grounded approach was employed to explore and categorize themes surrounding how participants felt about the invasive application and/or privacy policy they were shown. The process resulted in 6 identified themes. The codebook is provided in Table 4.1, which contains an overview of the response themes with an example from the data. These data were also used to answer **RQ₂**.

The 31 qualitative responses were initially coded for tonal valence (i.e., positive, negative, neutral tone) and then by thematic responses. A response with positive tone indicated that the participant supported the application, demonstrated interest in the application, and/or felt the need to share their desire to use the application if it were available. A response with negative tone indicated that the participant did not support the application, demonstrated concern with the

application or its features, and/or felt the need to share their distaste with the applications existence. A response with neutral polarity was one that was either vague and/or lacked a clear opinion of the application. Once these comments were categorized by tonal polarity, their frequencies were tallied. The resultant frequencies are as follows: Of the 31 qualitative responses, most were negative (35.4%; $n = 11$) or neutral (38.7%; $n = 12$), with 25.8% ($n = 8$) being positive.

A content analysis on the 31 qualitative usability responses was conducted. Tonal responses were analyzed to explore participants' reactions to the application and privacy policy. Tonal responses were relatively evenly distributed among being negative ($n = 11$; 35%), neutral ($n = 12$; 39%), and positive ($n = 8$; 26%). This indicates that participants' reactions were relatively mixed. The thematic content analysis yielded six themes encompassing the most frequent kinds of responses participants reported involving the applications and/or privacy policy. The most frequent response from the participants was that involving *data concerns* ($n = 11$, 35%), with the rest being relatively evenly distributed among the five other themes (i.e., *additional information requests* [$n = 2$; 6.5%], *policy/notification language request* [$n = 5$; 16.1%], *simple opinion/intention* [$n = 5$; 16.1%], *technological feature concerns* [$n = 4$; 12.9%] and *utilitarian self-reflection* [$n = 4$; 12.9%]). Eight of the participants who left comments regarding data concerns were shown the health application, five of which were shown the picture policy. This indicates that, when presented with a simplified privacy policy (with pictures) for a health-related application, there are some initial concerns regarding data collection.

The frequencies of consent across conditions support these findings, as well. While over half of those shown a privacy policy consented to use the application (without taking into account the 10 participants who consented *after* being shown the full policy), there were three instances where there were more participants who did not consent rather than consent, all of which involved the health application. In the partial health policy condition, over half of those who opted into reading the full privacy policy did not consent to use the application. In the picture

health condition, there were slightly more individuals who did not consent to use the application than those who consented. Of the few who opted to reading the full policy in this condition (i.e., health picture), *none of them consented to use the application*. This indicates a unique trend among those presented with a condensed policy and/or policy containing pictures for a health application: Participants seem to be concerned enough about the health application to not consent and opt out of the opportunity to use that application.

4.4 Synopsis

The present study found several key results. The first hypothesis in the present study was not supported; it was found that there was no relationship between one's awareness of mediated privacy and awareness of the persistence affordance. Instead, it was found that a positive relationship existed between awareness of privacy and awareness of visibility and encryption affordances. In other words, participants who reported to be aware of and concerned about their online privacy were likely to also report a knowledge of their online presence being visible to others (even outside of their social networks) and/or knowing of/having used encryption tools that are specifically for masking one's online presence. This finding also answered the first research question, that asked which mediated affordance (between visibility, persistence, and encryption) was correlated with positive awareness of privacy. Thus, the affordances with the most significant relationship to awareness of privacy were encryption and visibility.

With regard to H_2 , it was found that a positive relationship existed between awareness of mediated privacy and awareness of surveillance. This means that participants who reported to be aware of and concerned about their online privacy were also likely to report being aware of and concerned about online surveillance.

Finally, the final research question asked about the relationship between the modality of an invasive application's privacy policy and one's intentions to use that application and their awareness of online privacy and online surveillance after reviewing that privacy policy. Although it was found that there were no significant main effects between the kinds of policies shown and

one's self-reported awareness of online privacy and surveillance after viewing the privacy following, there were two significant results found in the post hoc tests. Individuals who were shown no privacy policy at all reported greater concerns for their online privacy than those who were shown a privacy policy containing imagery for an application that offers personalized services in exchange for data. Second, individuals who were shown a privacy policy containing pictures for a health application that requires one's data reported a greater concern for their online privacy than those shown a privacy policy containing images for an application that offers personalized services in exchange for data.

The post hoc content analysis supports this finding, as eight participants whose qualitative responses were concerned with the data collection aspect of the application were shown the health application's privacy policy that contained pictures. This indicates that, when participants were presented with a simplified privacy policy for a health-related application, they had some initial concerns regarding data collection. This finding is also supported when taking into account the frequencies of those who consented across the multiple experimental conditions of this study. Although most participants consented to use the application overall, the few instances of individuals *not* consenting in greater numbers than consenting participants occurred amongst those who were shown the health application's partial and picture policy.

Table 4.1

Codebook of Themes with Message Examples

Theme Name	Theme Description	Exemplar
Data Concerns	The general topic of the application's data collection/sharing aspect	"I chose that I wouldn't consent solely because I don't think I'd be comfortable with the app accessing my social media as I don't see a reason that it would need to."
Additional Information Requests	Uncertainty surrounding the application to the point of explicitly asking for more information, such as being unsure of what the purpose of the application	"I would need to read up more on what it offers but it sounds like a good idea."
Policy/Notification Language Request	Feedback and/or requests for modifying the application's privacy policy and/or notification	"Maybe add more info about which brand of item is being 'dropped'"
Simple Opinion/Intention	Focuses on the participant's opinion of/intention to use the application without justification as to why.	"This is a great idea!"
Technological Feature Concerns	Concerns related to specific technological features of the application outside of its data collection requests	"I usually don't like to turn on GPS."
Utilitarian Self-Reflection	Focuses on participants' utilitarian needs in relation to the application and/or self-reflection regarding the fit of the app into their lifestyle	"I am probably out of the age range for the use of this app. I have a sone[sic] that uses Drops for several items he has purchased. Good luck with your app!"

CHAPTER 5. DISCUSSION

Communication research lacks contemporary explanation for what privacy *is* beyond interpersonal phenomena (e.g., CPM; Petronio, 2013). Although theoretical frameworks involving media use (e.g., MAIN; Sundar, 2008) contain rich predictions and conditions regarding when and how a user might adopt a new technology, these models do not yet contain discourse as it pertains to user privacy. The novel coronavirus (COVID-19) and the resultant pandemic have presented a unique opportunity to examine privacy and its related variables, especially given the possibility of employing technologies that depend on citizens' data to limit the spread of the virus (Byford, 2020). Beyond the context of COVID-19, modern technological advances and social media platforms require users to consent and hand over their personal data in exchange for access. Thus, questions regarding data collection become intertwined with concerns related to privacy (e.g., Cheung et al., 2016), surveillance (e.g., Martin et al., 2016), and citizens' legal rights (Sirota, 2019) as well as more pertinent with the release and adoption of new technologies.

The present study was framed to address several privacy-related issues. The first major thrust was to explore which kinds of technological affordances were associated with greater awareness of privacy. Next, the study sought to understand the relationship between privacy and surveillance. The final area of focus questioned how the modality of a privacy policy factored into individuals making privacy decisions. The overarching intention of this study is that it could lay groundwork for a contemporary and timely discussion of privacy issues as it relates to computer-mediated behavior.

5.1 Overview and Explanation of Hypotheses/Research Questions

5.1.1 H₁, RQ₁: Privacy Awareness and Awareness of Affordances

The first hypothesis (H₁) posited that awareness of mediated privacy correlated negatively with awareness of privacy affordances. In other words, the more one was aware of their online privacy, the less aware they were in perceiving (and possibly utilizing) technological affordances related to new media and technologies. Several justifications exist within the literature for this hypothesis to be supported, be it related to the privacy paradox impacting users' online behaviors (Barnes, 2006; Quinn, 2016), users overestimating their online invulnerability (Shin et al., 2012), or users being cynical and/or apathetic when presented with the opportunity to proactively protect their online privacy (Hargittai & Marwick, 2016). However, the present study found conflicting results.

The resultant correlations employed in the present study did not support this hypothesis. While the results might be surprising given the ample literature supporting the notion of users failing to acknowledge their abilities to utilize affordances that can protect their privacy, a more thorough explanation can be found by discussing the results found from answering the study's first research question (RQ₁) of which technological affordances (of visibility, persistence, and encryption) were associated with greater awareness of privacy.

The present study found that a significant, weak, but positive, relationship existed between participants' awareness of mediated privacy and their awareness of visibility and encryption. The study also found that no significant relationship existed between participants' awareness of mediated privacy and their awareness of persistence. This implies that the more a participant was aware of their privacy, the more they were aware of being found on social media and/or aware of/currently employed specific technological affordances that feature encryption, thus protecting their privacy more than if they had not used considered using these affordances.

Although these findings might contrast with H_1 , there is much to unpack regarding how participants in this study consider affordances related to social media and new technologies.

Visibility is an affordance that is described as being able to selectively display oneself in an online setting, control how information is displayed to other users, and/or control being seen as offline or online (Evans et al., 2017; Siegert & Löwstedt 2019). The positive relationship that existed in the present study implies that the more aware one was of their online privacy, the more they knew of and/or utilized features that increased/decreased the visibility of their online presence. Within the context of privacy discourse, this could also refer to the default nature of one's online profile as being public or private and/or restricting the kinds of content that others can see. This finding is relatively unsurprising, as it would make sense for one who is concerned about their privacy to restrict their online presence and/or control who can see their online profiles. Control over information and information boundaries is a key facet of privacy as it is defined in the literature (Westin, 1967; Altman, 1975, 1977; Petronio, 2002, 2013), so seeing a positive relationship between controlling an online profile's information and concern about privacy makes logical sense. Furthermore, prior research has indicated that users make conscious decisions about who to become friends with, add, and/or follow on social media because of privacy concerns (Ampong et al., 2018; Child et al., 2012; Choi & Bazarova, 2015; Ellison et al., 2011; Quinn, 2016). The present study lends support to this literature in the sense that users are *cognizant* of social media's ability to limit content and network visibility. While this study does not explicitly support the notion of individuals adjusting their visibility online for the outcome of privacy, the findings indicate a possible perception and/or behavioral connection between privacy-conscious users and users who actively monitor and utilize their online visibility.

The encryption affordance utilized in this study has not typically been discussed in previous affordance literature (e.g., Evans et al., 2017). Instead, encryption-related affordances tend to exist in the literature discussing their utilization and efficacy in applications (e.g., WhatsApp; Santos & Faure, 2018). Encryption measures can be linked to utilizing end-to-end

encryption and/or employing a virtual private network (VPN) to browse the Internet. The positive relationship that existed in the present study implies that the more aware one was of their online privacy, the more they knew of and/or utilized features that encrypted their online presence. Within the context of privacy discourse, this could also refer to users turning to services specifically designed to preserve one's online privacy. This finding is also unsurprising on a surface level, as applications that feature these kinds of tools have existed as alternatives to mainstream services, such as the case of WhatsApp. This means that it is likely that only individuals who *knew* about specific encryption tools (e.g., end-to-end encryption), were concerned about their online presence to learn about these tools, and actively utilized them (as their specific purpose is for protecting one's online privacy). Although popular messaging services (e.g., Apple's iMessage, Google's Google Messages) are beginning to adopt end-to-end encryption in their applications and make them available for users (Doffman, 2020a; Hesse, 2020), there is a greater barrier to entry in that most users have to *opt in* to utilizing these affordances rather than having them automatically available as a default option. While this study does not explicitly support the notion of individuals seeking out encryption services for the outcome of privacy, the findings indicate a possible connection between privacy-conscious users and users who actively know of and/or turn to services that feature encryption mechanisms.

Persistence is an affordance that has described the *content* of one's online presence, specifically with regard to that content being able to be archived for future reference (Ellison et al., 2015) and/or durable to the point of that content being able to retain its integrity for others to interpret at any time, at a later time (Treem & Lombardi, 2012). Within the context of this study, knowledge of persistence existed as being aware of or concerned about users utilizing the screenshot function to preserve their own and/or other users' social media content. The present study found *no* significant relationship between awareness of one's privacy and awareness of the persistence affordance. This finding is inconsistent with prior privacy research on social media. A common concern among young adults and teenagers on social media is that their families can see,

and easily reference, their online behaviors; addressing this concern requires users to face the existence of social media persistence and actively edit/delete content that might be unsavory in the eyes of one's *Yia Yia* (Child & Westermann, 2013). This finding becomes less surprising considering the most popular forms of social media used by participants in this study. The overwhelming majority (over 90%!) of the participants in this study reported that they used Snapchat and/or Instagram. At the time of writing, both of these applications prominently feature the ability to directly send self-destructing messages and/or images to another, sharing sequences of images/videos (i.e., *Stories*) that other users can opt into viewing that expire after a certain amount of time, as well as *private Stories* that are only viewable by others that the user specifically selects (Bradford, 2018; Delfino, 2019). In other words, these applications preemptively resolve the concern of persistence by making non-permanent forms of communication the default means of communicating with other users. Thus, the lack of relationship between participants' self-reported awareness of privacy and awareness of persistence lend support to the idea that young adults have moved on to using non-permanent forms of social media where persistence is not a primary concern, if at all.

Another explanation for the lack of relationship between the study's participants' self-reported awareness of privacy and awareness of persistence can be explained when taking into account the relationship between participants' awareness of privacy and awareness of encryption. These encryption tools, be it proxies, VPNs, and end-to-end encryption, allow for a user to anonymize their web presence in the sense that their activity is encrypted, hashed (i.e., anonymized), forwarded to other random data stations, and then decrypted once it reaches its final destination (Montieri et al., 2018). This means that these tools provide users with the ability to mask their online presence, thus preemptively addressing a concern of their content persisting. If it is exceedingly difficult to trace content back to its source thanks to encryption tools, then there is little reason for a user to be actively concerned about their content persisting in an online context.

In sum, the answer to the study's first research question is as follows: awareness of visibility and encryption are nearly equally correlated to awareness of privacy. Although the correlation between encryption and privacy is *slightly* stronger than visibility and privacy, both correlations have a negligible difference when both correlation values are well in the region of a *weak* relationship.

5.1.2 H₂: Privacy Awareness and Awareness of Surveillance

The second hypothesis (H₂) posited that awareness of mediated privacy correlated positively with awareness of surveillance. In other words, the more aware of/concerned a participant was about their online privacy, the more aware of/concerned a participant was about online surveillance. The resultant correlation supported this hypothesis to a significant extent. This finding is consistent with surveillance literature that bemoaned the lack of privacy in public spaces (e.g., airports; Adey, 2006), the workplace (Kizza & Ssanyu, 2005; Lim, 2002; Mujtaba, 2003), in online settings (Caluya, 2010), or even by proxy thanks to amateur recording (i.e., an individual is technically under surveillance in a video posted to social media even if they are in the background of that video; Koskela, 2004, 2009). On face, this positive relationship makes sense: If one is concerned about being under surveillance, they are most likely concerned about their privacy being invaded because they are being watched, too. Another explanation for this significantly strong relationship could exist when the privacy paradox and culture of surveillance are considered together. Prior research has indicated that our behaviors drastically change when we are suddenly made aware of being under surveillance (Martin et al., 2016; Sarpong & Rees, 2014). Given that individuals are apathetic about their privacy until something tangible occurs that violates that privacy (Hargittai & Marwick, 2016), it would make sense for that apathy to occur when under *constant* surveillance rather than *sudden* surveillance. The present study lends support to the notion that privacy concerns and surveillance concerns are intertwined to a certain extent: these variables are related in the sense that users face the concerns retroactively rather than proactively.

5.1.3 RQ₂: Privacy Policy Modality and Privacy Decisions

The study's second research question (RQ₂) sought to understand the relationship between the modality of a privacy policy and awareness of surveillance, intentions to use an invasive application, and awareness of privacy. As this question was answered using mixed methods, there is much to interpret.

The first 2x3 factorial ANOVA focused on the six experimental conditions and the usability subscale. This specific ANOVA was conducted because participants in the control condition did not see the usability scale; only participants who were shown an application and privacy policy in one of the six experimental conditions had the opportunity to answer the usability questions. The resultant ANOVA found no significant main effect between a participant shown a different type of application (i.e., health or personalization), a modality of privacy policy (i.e., full, partial, or picture), and intention to use an application. Individual differences between groups were found to lack significance, as well. At first glance, this might mean that users' intentions to use a privacy-invasive application is not predicted by the kind of application and how the consent documentation is presented. Given that consent processes are routinized to the point of users opting to skip past them entirely (Ploug & Holm, 2013), it would be plausible to interpret this finding as lax participants being unphased by privacy policies. Taken alone, modality might not matter. However, it would be dangerous to come to such a conclusion without examining the results from the second ANOVA.

The second 2x3x1 factorial ANOVA was conducted between the six experimental conditions, the control condition, and the privacy awareness subscale. All participants were shown the privacy awareness scale, thus an ANOVA involving all of the groups could be conducted. Consistent with the prior ANOVA, there was no significant main effect between the type of privacy policy displayed, the type of application displayed, and awareness of mediated privacy. This might mean that, similar to the prior interpretation, the type of application or privacy policy modality does not determine one's awareness of online privacy. This surface level

finding can be explained as an example of the privacy paradox in which participants report being aware of their privacy yet failing to act and preserve it (Barnes, 2006). For the case of this study, a significant effect could indicate a departure from this paradox; participants recognizing the privacy invasive nature of the application and reporting heightened awareness of privacy could indicate some effect coming from the privacy policy. This was not the case here.

The post hoc tests told a slightly different story, however. Participants in the control condition reported greater awareness of privacy than those in the personalization picture policy condition. In other words, this means that individuals shown no privacy policy reported greater concerns about their privacy than those showing a condensed privacy policy containing images for an application that personalizes content for the user depending on their interests. Considering the personalization paradox, in which individuals knowingly give away their data (i.e., privacy) in exchange for personalized services (Aguirre et al., 2015), it would make sense for individuals to report less concern for their privacy if it means they get a unique experience. The present study's participants seemed to respond favorably in the form of having decreased privacy concerns when presented with an opportunity to have a tailored and customized experience. This finding is consistent with prior research in that customization and personalization were appealing enough for participants to look past privacy concerns (Sundar & Marathe, 2010). Moreover, it can be assumed that participants shown a condensed privacy policy containing pictures had the opportunity to understand the terms and conditions to the point of relaxing their vigilance and look forward to using an application fit for them. If this is the case, then it can also be assumed that the policy was instrumental in achieving a level of informed consent (Rossi & Palmirani, 2017). However, knowing the demographics of participants in this study being generally young adults completing this survey for college credit as well as how routinized consent procedures are (Ploug & Holm, 2013), it would be a significant (yet optimistic) stretch to assume that true consent was being obtained during the course of this study.

The continued post hoc tests also indicated that participants in the health picture policy condition reported greater awareness of privacy than those in the personalization picture policy condition. This means that those who were shown a health application with a summarized privacy policy containing pictures reported greater privacy concerns than those who were shown a summarized privacy policy for an application that tailors content for users depending on their interests. Like the previous post hoc results, this could be another example of the personalization paradox at play (Aguirre et al., 2015), in which participants' concerns were assuaged after knowing that an experience was being tailored. Modality might matter in this case. However, when taking into account the supplemental qualitative analyses, an alternative (and richer) explanation regarding this difference becomes clear.

The supplemental content analyses conducted on the usability and qualitative responses yield a deeper understanding as to why those in the health picture policy condition reported greater concerns than those in the personalization picture policy condition. First, when examining the differences in consenting frequencies among those in these conditions, the health picture policy condition featured the most instances of those not consenting rather than consenting. Of the few who were unsure and opted to read more in this specific condition, all of them did not consent. Conversely, of the few participants who opted to read more in the personalization picture condition, all of them consented to use this application. Although there were only eight participants who opted to read more in the policy condition (four in health, four in personalization), this polar trend of consenting versus not consenting is worth nothing when discussing concerns of the health application and the personalization paradox. This finding seems to be consistent with the anti-contact tracing sentiment that was reported in the media early on in the pandemic, where many individuals were quite hesitant about the efficacy and true intentions of the contact tracing efforts (Browne, 2020; Dev, 2020; Feibus, 2020). While this concern (and unwillingness) might not be stemming from the modality of policy itself, it can explain the lack of consenting participants in the health condition.

The content analysis of the application feedback explains some of this concern, too. While most comments were negative or neutral (i.e., vague or lacking a clear opinion of the application itself), the most common theme was that involving *data concerns*. Regarding their data, participants either explicitly described their intentions (i.e., “I will not openly give any app my personal information”) or their opinions regarding being watched altogether (i.e., “...however i have second thought about information release to third party services”). In the context of this study, this means that participants were most likely to express concerns about the application’s data collection features, its requiring user data, and/or concerns about what will be done with that data. This finding is consistent with research on cutting edge eHealth technologies that require participant data to function (Cheung et al., 2016). Although contact tracing is not a cutting-edge technology (see Bernard et al., 2018), the contexts of the COVID-19 pandemic and participants viewing an unreleased application would classify this pool of participants as potential early adopters when considering DoI (Rogers, 1962). For the case of this study, early adopters were quite concerned with the health application and their privacy to the point of opting out of using that new technology when presented with a privacy policy that was easier to understand. Thus, privacy risks posed a threat to the potential adoption of a new technology aimed at mitigating the spread of COVID-19 (a trend predicted by Bernstein [2006]).

The final 2x3x1 factorial ANOVA was conducted between the six experimental conditions, the control condition, and the surveillance subscale. All participants were shown the surveillance scale, thus an ANOVA involving all of the groups could be conducted. Consistent with the first ANOVA, there was no significant main effect between the type of privacy policy displayed, the type of application displayed, and awareness of surveillance. There were no significant differences within the individual groups, as well. While this might be an unexpected finding, the similarities between the first and third ANOVAs support the idea that there is significant overlap between awareness of privacy and surveillance. In the context of this study, if there were no main effects between privacy policy modality and privacy subscale, a similar lack

of main effects should exist between privacy policy modality. In this case, modality might not matter given the correlation between surveillance and privacy awareness.

Does the modality of a privacy policy matter among individuals making privacy decisions? The short answer is...*it depends*. On a surface level, the lack of main effects in most of the ANOVAs conducted in this study indicates that modality does not matter; users will routinely and blindly consent to use an application in a dismissive fashion (especially if its privacy policy is unstandardized, lacks plain language, and prevents individuals from becoming informed when consenting; Katulić & Katulić, 2018; Rossi & Palmirani, 2017). However, the individual differences that occurred between participants shown a health application with a policy containing pictures, personalization application containing pictures, and no privacy policy at all highlights a unique role a privacy policy played when participants were tasked with making a decision about their online privacy. In this study, the privacy policy commodified privacy in that participants had to answer the question of if their data was *worth* the exchange outlined in the policy (thus granting them potential access to the application). For the health application, a policy containing pictures (and assumedly allowing for greater comprehension) led to users feeling that their data was not worth access, even during the pandemic. For the personalization application, a policy containing pictures (and assumedly allowing for greater comprehension) led users to feel that exchanging their privacy for access to a new service *was worth it*. Thus, the modality of a policy *could* matter among users making decisions regarding their privacy, though it depends on the context.

5.2 Implications of Findings and Future Directions

The findings of the present study demonstrate potential for multiple social scientific fields that study privacy, policymakers seeking to implement data-informed improvements to privacy policies, and stakeholders seeking to address the privacy paradox. Although some of the findings in the present study lack significance, there is reason to consider the smaller findings with cautious optimism.

5.2.1 Theoretical Implication: Toward a contemporary conceptualization, and theory, of privacy.

Privacy remains a concept worth addressing (Margulis, 1977, 2003); at the very minimum, a theory of privacy should encompass contemporary communication behaviors as well as privacy issues of the status quo. Regardless of its prior framing as a human process (Altman, 1975, 1977), a communication tactic (Petronio, 2002), or a human right (Papacharissi, 2010; Sayre & Dahling, 2016; Warren & Brandeis, 1890), the present study contributes to an effort of elevating/revisiting the problem of privacy in the status quo. The definition of privacy (i.e., *mediated privacy*) that framed the present study was contingent on one having the right to conceal information so long as they remain in control of that information. Those who participated in this study tested this notion when they were presented with the option of giving away their data in exchange for access to a new application. In doing so, it can be argued that consenting to use either of the applications employed in the present study shaved away one's right to privacy in that control of one's personal data, even in the form of indicating one's favorite shoe brand, becomes a shared responsibility between a data owner (i.e., the user) and a data controller (i.e., the application collecting the data).

One goal of this study was to understand the relationship between privacy and surveillance, two concepts that are assumedly connected when examined at face value. Although Monahan's (2011) definition of surveillance frames it as an invasive process governing one's behavior (thus contrasting with several interpretations of privacy; cf. Altman, 1975, 1977), legitimizing its relationship with a related concept (i.e., privacy) is a step in the right direction for delineating these concepts in the future. The present study found that a positive and significant relationship existed between awareness of mediated privacy and awareness of surveillance. This finding is important for two reasons.

First, highlighting this relationship is important for privacy scholars seeking to position privacy alongside similar concepts. Surveillance literature has demonstrated that individuals change their behaviors when they are made aware of the act of surveillance taking place (Lim, 2002; Kizza & Ssanyu, 2005; Mujtaba, 2003). Knowing the positive relationship demonstrated in this study paves the way for opportunities to address underlying surveillance concerns, and in turn, privacy concerns. For example, scholars wanting to examine the effects of surveillance can now examine privacy awareness in their research. Second, the relationship between these two concepts noted in this study demonstrate a future need to differentiate these concepts for future research operationalization. For instance, if we are to consider Monahan's (2011) conceptualization, a future direction could be to understand the difference between *active* surveillance (e.g., being constantly monitored in the workplace; Kizza & Ssanyu, 2005) and passive surveillance (e.g., learning that one was under surveillance when they end up in the background of someone else's video posted on social media; Koskela, 2004, 2009). Both forms of surveillance can be associated with privacy risks outlined foretold by 6 (1998), but contemporary privacy issues could dictate which type of surveillance sparks more pressing privacy concerns, thus better defining privacy as it relates to contemporary privacy issues.

Future privacy research can benefit from the reflexive approach adopted in this study. boyd's (2012) recommendation of decentering the individual as the unit of analysis (as it pertains to privacy research) lacked a means of operationalization; the present study made an attempt at operationalizing that recommendation by examining privacy from the affordance theoretical perspective, which brought its own set of implications for media researchers.

5.2.2 Theoretical Implication: Reconsidering privacy from an affordance perspective.

Gibson's (1986) interpretation of an affordance is admittedly naturalistic when used to reference new media and technology phenomena. Contemporary communication affordance

research involving social media might examine how users interact with a social media platform (e.g., Aladwani, 2017) or how social media impacts behaviors (e.g., Rice et al., 2017). For the case of the present study, an affordance perspective examined what features offered by social media were related to awareness of privacy. The three affordances examined in the present study were *visibility*, *persistence*, and *encryption*.

A goal of this study was to understand which technological affordances were associated with greater awareness of privacy. It was assumed that, given the privacy paradox causing users to give away their privacy yet being concerned about it (Quinn, 2016) and individuals demonstrating apathy when presented with an opportunity to address their lack of privacy preservation (Hargittai & Marwick, 2016), participants in this study would indicate greater awareness of privacy and lesser awareness of technological affordances on social media that can be associated with privacy (i.e., a negative relation). The lack of support for **H₁** is important because it offers an alternative explanation for user behavior impacted by the privacy paradox. If users are aware of some technological affordances (as demonstrated in this study), yet concerned about their privacy, this indicates that users might not be apathetic. In fact, this disconnection between concern and action could be explained by something else altogether, such as a lack of knowledge. Future affordance research should examine that disconnection in attempt to explain the root causes of the privacy paradox.

Another important implication from this study can be found in the lack of a relationship between privacy awareness and awareness of the persistence affordance. *Persistence* is a social media affordance frequently discussed in computer-mediated communication (CMC) and social media literature relating to content being able to *persist* in the form of archived for future reference and retaining most of its structure, so its meaning is not misconstrued (Ellison et al., 2015; Treem & Leonardi, 2012). Although persistence itself might vary by platform and medium (Evans et al., 2017), the lack of a relationship between privacy awareness and visibility awareness marks a trend worth noting for future affordance literature: Persistence is becoming less of a

default and prominent affordance found on social media, and in turn, CMC. In the present study, the overwhelming majority of participants reported to use Snapchat and Instagram, two social media platforms that prominently feature ephemeral media in the form of self-destructing messages and images (Bradford, 2018; Delfino, 2019). Snapchat users circumvent the default notion of persistent media by sending a picture to someone else that can be viewed exactly once. Although a level of persistence still technically exists in the form of users utilizing the screenshot function of their devices when opening a self-destructing message, these users have to specifically opt into doing so by learning how to screenshot on their device, predict an incoming message to be valuable enough to be preserved via screenshot, and recognizing the fact that Snapchat notifies all parties in a conversation that a screenshot was taken (perhaps in an attempt to mitigate abusive behavior and encourage a reciprocal culture of engaging in ephemeral communication on the platform). This finding is important for a few reasons.

First, this finding demonstrates a need to reclassify persistence as an affordance that is no longer the default on contemporary social media platforms (cf. Evans et al., 2017). Given that new social media platforms are giving users more control over their data and how they interact with others through the introduction of new features (and their impacts on the average user), affordance literature *must* catch up and reclassify common/default communication/technological affordances offered by social media. Second, this finding demonstrates a need for a *new* affordance to be examined by the literature: *Evanescence*. Similar to face-to-face (FtF) communication, which is fleeting by default in the sense that all human participants in a communication interaction lack the ability to preserve the messages being exchanged without a recording device, evanescence could refer to a unique type of ephemeral CMC where the message *sender* dictates ephemerality of the message prior to sending it to someone else (who might or might not have the capability of preserving the messages being sent).

The present study lacked a singular overarching theoretical framework that framed the study based on a singular line of literature. Instead, it incorporated several theoretical

backgrounds to be reflexive while also offering competing explanations for the paradoxes of privacy and personalization in the status quo.

5.2.3 Theoretical Implication: Reconsidering privacy within the contexts of DoI and MAIN.

Diffusion of Innovation (DoI) and the MAIN model are two sets of media use frameworks that attempt to predict when and/or why a new technology/media is adopted by an audience. For the case of DoI, this can help in classifying *kinds* of users and offer an explanation as to when users might adopt this new technology (thus predicting its success and eventual diffusion across a population; English, 2016; Rogers, 1962; Schwartz & Grimm, 2017). For the case of the MAIN model, this can help in classifying what *affordances* and/or heuristics might be appealing to users that encourages them to continue to use specific technologies or media forms (Sundar, 2008). While the present study did not have a specific goal framed around these theoretical frameworks, the findings yielded by the supplemental analyses, particularly the consent frequencies and content analyses, offer opportunities for media and privacy scholars to consider. The present study found that there were multiple instances where early adopters opted out of using a new *health* application that could be considered to be privacy invasive and this could be important for a number of reasons.

First, this finding demonstrates that an opportunity exists for these theories to be tested using technologies and media forms from multiple contexts beyond general media use, such as using new health technologies. While some literature exists briefly describing the thoughts of hesitant early adopters of new health technologies (Cheung et al., 2016), this hesitancy cannot be explained by DoI nor MAIN. Given the similar health hesitancy experienced by participants in this study, it is imperative for future research to address the contextual deficiency that exists from both DoI and MAIN. Second, the findings of this study indicate that these models need to clearly take privacy into account. Given that a relationship exists between privacy awareness and certain technological affordances, an opportunity exists in further understanding the role privacy awareness plays in media and technological adoption. The present study contains findings

consistent with prior *personalization paradox* research that hypothesizes and discusses how privacy awareness predicts attitudes of new technologies (Bernstein, 2006; Cho et al., 2020; Sundar & Marathe, 2010). While privacy might not be an outcome variable, it acts as a predictive variable worth exploring in future research on technological adoption and media diffusion.

While the present study offered much to communication theory and media use theories, there are practical implications related to privacy policy modalities that are worth noting for scholars, policymakers, and other stakeholders who have a vested interest in updating privacy policies to be compliant with contemporary legislation while also being data-informed.

5.2.4 Practical Implication: Much ado about privacy policies.

The privacy policy has become the focus of examination by both lawmakers and scholars alike. Privacy legislation such as the GDPR (GDPR, 2016) and CCPA (Sirota, 2019) has aimed to protect the privacy of citizens on multiple fronts, one of which being the standardization and clarification of privacy policies. Again, answering the question whether or not privacy policies actually *meet their goals of protecting privacy* is outside of the scope of this study. Instead, a goal of this study was to examine differences in *how* users interacted with several modalities of privacy policies. These manufactured policies were constructed to be consistent with prior recommendations of privacy researchers, in which policies should be summarized, contain pictures, contain clear language, and ensure that a level of informed consent can be met by the end user (Katulić & Katulić, 2018; Ploug & Holm, 2013; Rossi & Palmirani, 2017). Although there were virtually no main effects between participants' awareness of usability, privacy, surveillance and modality of privacy policy shown, the few significant individual differences noted in the present study are worth discussing.

First, it can be assumed that participants initially shown the picture policies and then opting to read the full policies for the health and personalization applications were able to comprehend the policies *just enough* to warrant a consistent trend of health participants *not consenting* and personalization participants *consenting* to use the application in an extreme

fashion. This bipolarity of consent did not occur in the partial policy condition. This finding is important for privacy researchers or policymakers who want to better understand how to raise comprehension levels and limit users from blindly consenting (see Rossi & Palmirani, 2017). However, future research should examine privacy policy modality further to gauge comprehension from users reading privacy policies that have been standardized with *informed* consent in mind. Second, the hesitancy among participants in the health subconditions (i.e., health picture, health partial) and their qualitative feedback regarding their data indicate that a level of user concern needs to be addressed by researchers, lawmakers, and developers of these *health* applications to allow for users to consent without concern. However, this might prove ethically difficult (see Pollach, 2005). Privacy policies and consent documentation require the use of plain language, *elaborated* procedures for addressing concerns, and *rich* and *detailed* descriptions of the legal and/or research processes that will be taking place. This could mean that *too much* information in health contexts might be raising an equal level of user concern as *too little* information. Thus, researchers, lawmakers, developers, and practitioners have an opportunity to reframe information on these privacy policies and consent documentation in a way that meets guidelines set forth by legal bodies, are ethically and morally consistent with health research, and assuage concerns users might have prior to reading that policy.

Outside of practical implications for privacy policies and privacy research, the present study's findings involving the *encryption* affordance offer implications for privacy researchers and developers to consider going forward.

5.2.5 Theoretical & Practical Implications: Encryption, end users, and you.

The *encryption* affordance discussed and analyzed in this study is not a technological affordance often discussed in affordance classification literature (e.g., Evans et al., 2017; Rathnayake & Winter, 2018). Instead, the present study operationalized measuring knowledge of encryption affordances by referencing mechanisms and processes that encrypt one's online presence in the status quo (e.g., Santos & Faure, 2018). The present study found that a positive

relationship existed between knowledge of encryption affordances and awareness of privacy. Knowing that these affordances have primarily existed as opt-in affordances for technologically savvy users, this finding is important for two reasons.

First, this relationship demonstrates that affordance classifications can be updated to include technological affordances *specifically* created for privacy. The encryption affordances referenced in this study (i.e., VPNs, end-to-end encryption, proxies) were comprised of mechanisms that were created and utilized *specifically* for masking one's online presence (thus allowing them to browse the web in a *private fashion*; Doffman, 2020a; Hesse, 2020; Santos & Faure, 2018). Thus, affordance classifications should be updated by media scholars to include affordances that involve outcome variables such as privacy. Second, given that *any* relationship exists, let alone positive, between knowledge of encryption affordances and awareness of privacy, this means that developers, privacy scholars, and legislators can safely assume that individuals are slowly becoming tech-savvy enough to at *least* recognize the existence and efficacy of these encryption affordances. This does not mean that messaging services and platforms should ease off making services such as end-to-end encryption available by default. The addition of making this feature the default form of messaging on mainstream messaging platforms such as Apple's iMessage (Doffman 2020a) and Google's Google Messages are a step in the direction of accounting for the average user being the weakest link in the cybersecurity chain (Culp, 2016). Developers and privacy scholars should consider allowing users to *opt out* of using these technologies (assuming that opting out of such an encryption mechanism provides a user with benefits in *very select* circumstances) rather than hoping that the users are smart enough and/or proactive to opt into such a service.

5.3 Limitations and Future Research

Although these results have been interpreted with optimism in a grim reality that features the privacy paradox, the present study has several limitations. First, the present study relied entirely on self-report mechanisms. Future privacy research could account for this limitation by

introducing another point of measurement, such as requesting individuals submit proof of their privacy settings.

Second, the population was sampled from a large Southern University, meaning that it is exceedingly difficult to make claims about *an average user*. Future research should consider sampling from multiple demographics for a more holistic understanding of average user behavior in mediated settings.

Third, although the affordance measures created for and utilized in this study had sufficient reliability, the submeasures themselves were comprised of very few items (in some cases, three items). In some cases, there were concerns regarding the measures, construct validity. For example, persistence is an affordance that manifests itself in fashions outside of the screenshotting social media content. Therefore, it would behoove future research to create an affordance measurement scale as a way to broaden affordance measures and include items that can measure these affordances in a variety of ways while also maintaining high reliability values.

Fourth, the study lacked a means of gauging the extent of participants' comprehension of the privacy policies themselves. There could have been situations where participants blindly scrolled to the bottom of the page in search of the "I consent" button. Although prior research recommends the use of short quizzes (e.g., Rossi & Palmirani, 2017), no such comprehension check was in place. Future research on privacy policy modalities should include a comprehension check to account for such a limitation.

Fifth, the study's design was limited in its ability to account for privacy's nuance. Privacy policies are uniform in nature; they are constructed in compliance with ethical, legal, and moral obligations (Angulo et al., 2012; Ploug & Holm, 2013; Pollach, 2005). Privacy, as well as the privacy paradox, require significant levels of nuance that are unable to be accounted for in a rigid study (such as this one); privacy is studied in a significant number of contexts. When trying to leverage results from the present study in relation to other contextual privacy research, cross comparisons become difficult to make. In short, it becomes difficult to compare the results from

this study to another privacy study given the lack of uniformity of privacy research. To account for this limitation, it is recommended that *specific* contexts of privacy are focused on for a holistic understanding of how privacy operates *within that specific context*.

Finally, the study was limited in its narrow ecological validity. Participants technically knew they were contributing to research all along, as they were participating in research for course credit and had to read through a consent document that reminded them of their research participation. Although IRB-approved deception measures were implemented in an attempt to simulate a consent obtaining process, there very well could have been users who “consented” on the fake application because they knew their data was being collected. To account for this limitation, future research should consider the route of participant observation and/or the use of psychophysiological measures that track movement (e.g., eye tracking) to gauge the attention of participants and determine if they’re actually reading and comprehending the content.

5.4 Summary and Conclusion

The purpose of this study was to better understand the extent to which one perceives their policy and affordances related to individuals perceiving their privacy when presented with privacy policies of different modalities, as well as understand the relationship between individuals’ self-reported privacy beliefs and their awareness of online privacy. The goal of this study was to contribute to a body of literature that lacks contemporary explanations for privacy and reflexive approaches for addressing problems related to online privacy. Although it was found that there were no main effects between modality of policy shown and awareness of surveillance nor privacy, there were significant individual differences between two conditions that were shown a privacy policy containing pictures. Furthermore, it was found that a positive relationship existed between awareness of privacy and surveillance as well as awareness of privacy and awareness of visibility and encryption. While the findings in this study were limited by multiple factors, the present study offers implications for scholars, legislators, and other stakeholders who seek to preserve the privacy of the end user. The problem of privacy will not be

solved over the course of a single dissertation project, nor is it technically dead. Instead, the boundaries of privacy are constantly evolving in tandem with technological advances; future privacy research should be mindful of these findings and evolve in tandem with privacy's boundaries.

APPENDICES

APPENDIX 1. STUDY MEASURES

Unless otherwise noted, all items will be presented in a 7-item Likert-type (strongly disagree to strongly agree) scale.

[INSERT CONSENT LETTER HERE]

Do you consent to participate in this study?

Yes No

[page break]

Text

Before we begin this study, we'd love to get to know a little more about you.

Sociodemographics

How old are you?: _____

What is your gender? M/F/FtM/MtF/Nonbinary/Other: _____

What is your sexuality?: Heterosexual, G, L, B, A, Other: _____

What is your ethnicity?: American Indian/Alaskan Native, Asian/Pacific Islander, Black/African American, Hispanic/Latino, White/Caucasian, Other: _____

What is your relationship status?: Single never married, in a committed relationship, domestic partnership, married, widowed, divorced.

What is your current class standing?: Fresh, Soph, Jr, Sr

What is your political alignment?: Liberal, Conservative, Independent, Unsure, Other: _____

How many apps have you installed on your phone? (Please estimate) _____

Which kind of smartphone do you have? Android, iOS, I do not have a smartphone

Social Media Use

Which social media platforms do you use? Please check all that apply: Facebook, Snapchat, Reddit, Twitter, TikTok, Instagram, LinkedIn, tumblr, Other: _____, None of the above

How often do you check your social media? Hourly, Multiple times a day, A few times during the day, at least once a day, a few times a week, a few times a month, less than a few times a month

[page break]

Text

Thank you, once again, for participating in this study! We are in the process of testing a brand new smartphone application, and we would love your input! On the next page, you

will learn about this new application. Then, we will show you its privacy policy. Then, we will ask you for your feedback on this application. Please click the arrow below to continue.

>>

[page break]

Qualtrics will then randomly assign participants to one of the following seven conditions with the QUOTA logic to ensure that all conditions have a near-equal amount of participants.

Condition 1: Health

The application is called **CoronaWatch**. This application will **continuously** have access to your current location (**GPS**), your device's battery life, your network information (**WiFi**), as well as monitoring your device's **Bluetooth**. As it tracks your daily routine, it will also connect to other students' devices (via **Bluetooth**). By signing up to use this application, you will be asked to consent to receive advertisements and announcements from the University.

In a scenario where you come in contact with someone who tests positive for COVID-19, **CoronaWatch** will alert you with a notification (see image below). You will then be directed to immediately self-isolate. Opening the notification will show you further instructions. Please see the notification below, as we will be asking you for feedback on the app's notifications.

[image goes here]

>>

Here is the application's privacy policy.

Subcondition A: Full Policy

SubCondition B: Partial Policy

Subcondition C: Picture Policy

>>

Condition 2: Personalization

The application we are creating is called **DropWatch**, an application for automatically entering exclusive product release raffles (aka "Drops"). This application will need an **Internet connection (WiFi or mobile data)** as well as your **GPS** to show you content that is relevant to your interests and your location. By signing up to use this application, you will be asked to consent to receive announcements and advertisements from

DropWatch and our advertising partners. When you first open the application, you will be asked to select your favorite clothing brands. When your selected clothing brands announce an upcoming drop, **DropWatch** will notify your automatic entry in that drop with a notification (see image below). Opening the notification will show you more information about the Drop. Please see the notification below, as we will be asking you for feedback on the app's notifications."

[image goes here]

>>

[page break]

Subcondition A: Full Policy

SubCondition B: Partial Policy

Subcondition C: Picture Policy

Condition 3: Control

We're sorry, but the application is not available to be shared yet. We're going back to the drawing board to come up with the next great thing! Please proceed to the next part of the survey.

USABILITY ITEMS (Control will not be given these items)

Text

We would love your feedback on this application! Please indicate your agreement with the following statements.

I think that this application is something I will need.

I plan on installing this application on my smartphone.

The app's notification contains just enough information for me to understand.

If I received this notification on my smartphone, I will open it for more information.

Written out feedback will be used in content analysis

If you have any other feedback you want to give us, please enter it in the text box below.

[insert text box here]

>>

[page break]

Text

Thank you for your feedback! We really appreciate it! Next, we would like to ask you some more questions. (ORDER OF QUESTIONS TBA)

Privacy Awareness (Aldhafferi et al., 2013; Dinev & Hart, 2005; Koohang, 2017; Krasnova et al., 2009)

Concern Subscale

It bothers me when social media sites ask me to provide personal information.
When social media sites ask me for personal information, I sometimes think twice before providing it.
I am concerned that social media sites are collecting personal information about me.
I am concerned about providing my information to apps because of what others might do with my information.
I am concerned about submitting my information to apps because it could be used in a way that I did not foresee.
I am often concerned that a social network provider could store my information for the next couple of years
Every now and then I feel anxious that a social network provider might know too much about me.

Awareness Subscale

I am worried about the misuse of my personal information
It is ok for my account provider (such as Facebook) to share my profile information with other websites **
I do not mind adding an unknown person as a friend **
I use real personal information on my social media account **
I am comfortable with strangers seeing my profile **

Knowledge and Utilization of Affordances (Evans et al., 2017; Miller et al., 2019; Santos & Faure, 2018; Siegert & Löwstedt 2019).

Visibility (see Evans et al., 2017)

I know how to adjust the visibility of my social media profiles.
I have adjusted the visibility of my social media profiles.
I know how to restrict my social media posts so that only a select number of people can see it.
I have restricted my social profile so that only a select number of people can see it.

Persistence (Evans et al., 2017; Siegert & Löwstedt, 2019)

I have taken screen shots of my friends' social media posts.
I know that some of my friends have taken screen shots of my social media posts.
Before I post something to social media, I worry about who might take a screen shot of my post. **

I prefer to use non-permanent forms of social media, such as Snapchat and Instagram Direct.

I prefer to use permanent forms of social media, such as Facebook and Twitter. **

I prefer to use forms of social media that lack public profiles. **

Other tech affordances (Santos & Faure, 2018)

I prefer to use messaging applications featuring end-to-end encryption.

I have used apps that feature end-to-end encryption.

I prefer to use a virtual private network (VPN) when I connect to the Internet.

I prefer to connect to the Internet through a proxy server.

Awareness of Surveillance

I have said something and have received an advertisement about it shortly after.

I am aware that tagging myself at a location can make my information public.

I think that there are too many opportunities for someone to be recorded.

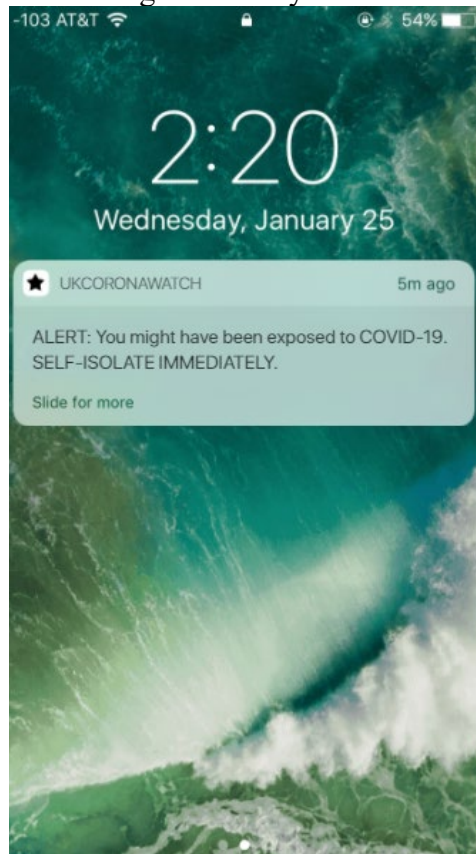
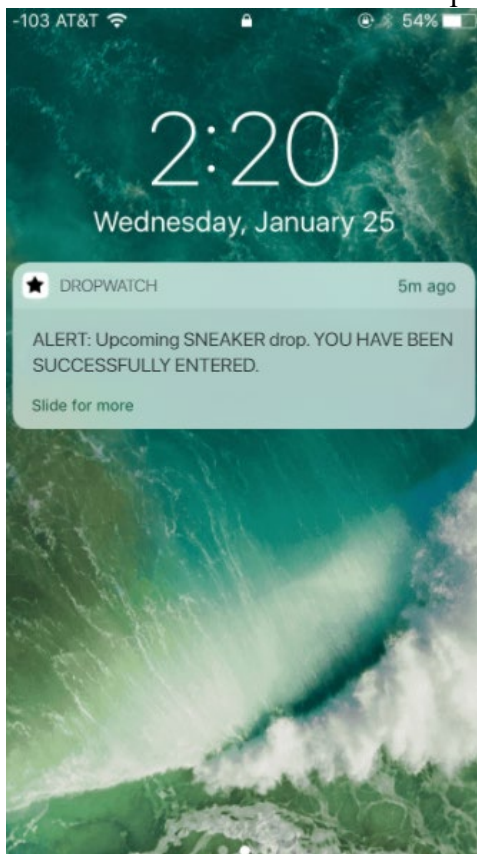
I think that there are too many types of ways to watch someone.

It is too easy to find someone on the Internet.

I do not mind being watched. **

I am concerned that I am being recorded.

**Indicates item was removed prior to running scale analyses.



APPENDIX 2 STIMULI USED (PRIVACY POLICIES)

CONDITION: FULL POLICY

Privacy Policy

(If you are a user having your usual residence in the US)

Last update: January 1, 2020.

The Platform is provided and controlled by Watch Inc. (“Watch”, “we” or “us”). We are committed to protecting and respecting your privacy. This Privacy Policy covers the experience we provide for all of our users.

Capitalized terms that are not defined in this policy have the meaning given to them in the Terms of Service.

What information do we collect?

We collect information when you create an account and use the Platform. We also collect information you share with us from third-party social network providers, and technical and behavioral information about your use of the Platform. More information about the categories and sources of information is provided below.

Information you choose to provide

For certain activities, such as when you register, use the Platform, or contact us directly, you may provide some or all of the following information:

- Registration information, such as age, username and password, language, and email or phone number
- Profile information, such as name, social media account information, and profile image
- Your opt-in choices and communication preferences
- Information to verify an account
- Information in correspondence you send to us
- Information you share through surveys such as your gender, age, likeness, and preferences.

Information we obtain from other sources

We may receive the information described in this Privacy Policy from other sources, such as:

Social Media. if you choose to link or sign up using your social network (such as Facebook, Twitter, Instagram, or Google), we may collect information from these social media services, including your contact lists for these services and information relating to your use of the Platform in relation to these services.

Third-Party Services. We may collect information about you from third-party services, such as advertising partners and analytics providers.

Others Users of the Platform. Sometimes other users of the Platform may provide us information about you, including through customer service inquiries.

Other Sources. We may collect information about you from other publicly available sources.

Information we collect automatically

We automatically collect certain information from you when you use the Platform, including internet or other network activity information such as your IP address, geolocation-related data (as described below), unique device identifiers, and Cookies (as defined below).

Usage Information

We collect information regarding your use of the Platform. We also link your subscriber information with your activity on our Platform across all your devices using your email, phone number, or similar information.

Device Information

We collect information about the device you use to access the Platform, including your IP address, unique device identifiers, model of your device, your mobile carrier, time zone setting, screen resolution, operating system, app and file names and types, keystroke patterns or rhythms, and platform.

Location data

We collect information about your location, including location information based on your SIM card and/or IP address. With your permission, we may also collect Global Positioning System (GPS) data.

Metadata

When you provide information to us, you automatically upload certain metadata that is connected to the User Content. Metadata describes other data and provides information about your User Content that will not always be evident to the viewer. In connection with your User Content the metadata can describe how, when, and by whom the piece of User Content was collected and how that content is formatted. It also includes information, such as your account name, that enables other users to trace back the User Content to your user account. Additionally, metadata will consist of data that you chose to provide with your User Content, e.g. any hashtags used to mark keywords to the video and captions.

Cookies

We and our service providers and business partners use cookies and other similar technologies (e.g. web beacons, flash cookies, etc.) (“Cookies”) to automatically collect information, measure and analyze which web pages you click on and how you use the Platform, enhance your experience using the Platform, improve the Platform, and provide you with targeted advertising on the Platform and elsewhere across your different devices. Cookies are small files which, when placed on your device, enable the Platform to provide certain features and functionality. Web beacons are very small images or small pieces of data embedded in images, also known as “pixel tags” or “clear GIFs,” that can recognize Cookies, the time and

date a page is viewed, a description of the page where the pixel tag is placed, and similar information from your computer or device. To learn how to disable Cookies, see the “Your choices” section below.

Additionally, we allow these service providers and business partners to collect information about your online activities through Cookies. We and our service providers and business partners link your contact or subscriber information with your activity on our Platform across all your devices, using your email or other log-in or device information. Our service providers and business partners may use this information to display advertisements on our Platform and elsewhere online and across your devices tailored to your interests, preferences, and characteristics. We are not responsible for the privacy practices of these service providers and business partners, and the information practices of these service providers and business partners are not covered by this Privacy Policy.

We may aggregate or de-identify the information described above. Aggregated or de-identified data is not subject to this Privacy Policy.

How we use your information

As explained below, we use your information to fulfill and enforce our [Terms of Service](#), to improve and administer the Platform, and to allow you to use its functionalities. We may also use your information to, among other things, show you suggestions, promote the Platform, and customize your ad experience.

We generally use the information we collect:

- to fulfill requests for products, services, Platform functionality, support and information for internal operations, including troubleshooting, data analysis, testing, research, statistical, and survey purposes and to solicit your feedback
- to customize the content you see when you use the Platform. For example, we may provide you with services based on the country settings you have chosen or show you content that is similar to content that you liked or interacted with
- to send promotional materials from us or on behalf of our affiliates and trusted third parties
- to improve and develop our Platform and conduct product development
- to measure and understand the effectiveness of the advertising we serve to you and others and to deliver targeted advertising
- to make suggestions and provide a customized ad experience
- to support the social functions of the Platform, including to permit you and other users to connect with each other through the Platform and for you and other users to share, download, and otherwise interact with User Content posted through the Platform
- to use User Content as part of our advertising and marketing campaigns to promote the Platform
- to understand how you use the Platform, including across your devices

- to infer additional information about you, such as your age, gender, and interests
- to help us detect abuse, fraud, and illegal activity on the Platform
- to ensure that you are old enough to use the Platform (as required by law)
- to communicate with you, including to notify you about changes in our services
- to announce you as a winner of our contest, sweepstakes, or promotions if permitted by the promotion rule, and to send you any applicable prizes
- to enforce our terms, conditions, and policies
- consistent with your permissions, to provide you with location-based services, such as advertising and other personalized content
- to inform our algorithms
- to combine all the information we collect or receive about you for any of the foregoing purposes
- for any other purposes disclosed to you at the time we collect your information or pursuant to your consent.

How we share your information

We are committed to maintaining your trust, and while Watch does not sell personal information to third parties, we want you to understand when and with whom we may share the information we collect for business purposes.

Service Providers and Business Partners

We share the categories of personal information listed above with service providers and business partners to help us perform business operations and for business purposes, including research, payment processing and transaction fulfillment, database maintenance, administering contests and special offers, technology services, deliveries, email deployment, advertising, analytics, measurement, data storage and hosting, disaster recovery, search engine optimization, marketing, and data processing.

Within Our Corporate Group

We may share your information with a parent, subsidiary, or other affiliate of our corporate group.

In Connection with a Sale, Merger, or Other Business Transfer

We may share your information in connection with a substantial corporate transaction, such as the sale of a website, a merger, consolidation, asset sale, or in the unlikely event of bankruptcy.

For Legal Reasons

We may disclose your information to respond to subpoenas, court orders, legal process, law enforcement requests, legal claims, or government inquiries, and to protect and defend the rights, interests, safety, and

security of Watch Inc., the Platform, our affiliates, users, or the public. We may also share your information to enforce any terms applicable to the Platform, to exercise or defend any legal claims, and comply with any applicable law.

With Your Consent

We may share information for other purposes pursuant to your consent or with your further direction.

If you access third-party services, such as Facebook, Google, or Twitter, to login to the Platform or to share information about your usage on the Platform with others, these third-party services may be able to collect information about you, including information about your activity on the Platform, and they may notify your connections on the third-party services about your use of the Platform, in accordance with their privacy policies.

If you choose to engage in public activities on the Platform, you should be aware that any information you share may be read, collected, or used by other users. You should use caution in disclosing personal information while engaging. We are not responsible for the information you choose to submit.

Your Rights

You may submit a request to access or delete the information we have collected about you by sending your request to us at the email or physical address provided in the Contact section at the bottom of this policy. We will respond to your request consistent with applicable law and subject to proper verification. And we do not discriminate based on the exercise of any privacy rights that you might have.

Your Choices

- You may be able to refuse or disable Cookies by adjusting your browser settings. Because each browser is different, please consult the instructions provided by your browser. Please note that you may need to take additional steps to refuse or disable certain types of Cookies. For example, due to differences in how browsers and mobile apps function, you may need to take different steps to disable Cookies used for targeted advertising in a browser and to disable targeted advertising for a mobile application, which you may control through your device settings or mobile app permissions. In addition, your choice to disable cookies is specific to the particular browser or device that you are using when you disable cookies, so you may need to separately disable cookies for each type of browser or device. If you choose to refuse, disable, or delete Cookies, some of the functionality of the Platform may no longer be available to you. Without this information, we are not able to provide you with all the requested services, and any differences in services are related to your information.
- You can manage third-party advertising preferences for some of the third parties we work with to serve advertising across the Internet by clicking [here](#) and by utilizing the choices available at www.networkadvertising.org/managing/opt_out.asp and www.aboutads.info/choices.
- Your mobile device may include a feature that allows you to opt out of some types of targeted advertising ("Limit Ad Tracking" on iOS and "Opt out of Interest-Based Ads" on Android).
- You can opt out of marketing or advertising emails by utilizing the "unsubscribe" link or mechanism noted in marketing or advertising emails.

- You can switch off GPS location information functionality on your mobile device if you do not wish to share GPS information.
- If you have registered for an account you may access, review, and update certain personal information that you have provided to us by logging into your account and using available features and functionalities.
- Some browsers transmit "do-not-track" signals to websites. Because of differences in how browsers incorporate and activate this feature, it is not always clear whether users intend for these signals to be transmitted, or whether they even are aware of them. We currently do not take action in response to these signals.

Security

We use reasonable measures to help protect information from loss, theft, misuse and unauthorized access, disclosure, alteration, and destruction. You should understand that no data storage system or transmission of data over the Internet or any other public network can be guaranteed to be 100 percent secure. Please note that information collected by third parties may not have the same security protections as information you submit to us, and we are not responsible for protecting the security of such information.

Children

The privacy of users under the age of 13 ("Younger Users") is important to us. We provide a separate experience for Younger Users in the United States on the Children's Platform, in which we collect only limited information.

The Platform otherwise is not directed at children under the age of 13. If we become aware that personal information has been collected on the Platform from a person under the age of 13 we will delete this information and terminate the person's account. If you believe that we have collected information from a child under the age of 13 on the Platform, contact us.

Other Rights

Sharing for Direct Marketing Purposes (Shine the Light)

If you are a California resident, once a calendar year, you may be entitled to obtain information about personal information that we shared, if any, with other businesses for their own direct marketing uses. If applicable, this information would include the categories of customer information, as well as the names and addresses of those businesses with which we shared customer information for the immediately prior calendar year.

Content Removal for Users Under 18

Users of the Platform who are California residents and are under 18 years of age may request and obtain removal of User Content they posted by contacting us. All requests must be labeled "California Removal Request" on the email subject line. All requests must provide a description of the User Content you want removed and information reasonably sufficient to permit us to locate that User Content. We do not accept California Removal Requests via postal mail, telephone, or facsimile. We are not responsible for notices that are not labeled or sent properly, and we may not be able to respond if you do not provide adequate information. Please note that your request does not ensure complete or comprehensive removal of the material. For example, materials that you have posted may be republished or reposted by another user or third party.

Changes

We may update this Privacy Policy from time to time. When we update the Privacy Policy, we will notify you by updating the “Last Updated” date at the top of this policy and posting the new Privacy Policy and providing any other notice required by applicable law. We recommend that you review the Privacy Policy each time you visit the Platform to stay informed of our privacy practices.

Privacy Policy

(If you are a user having your usual residence in the European Economic Area (EEA) or the UK, or Switzerland)

Last updated: July 2020

Welcome to Watch (the “Platform”). We are committed to protecting and respecting your privacy and this policy sets out the basis on which we process any personal data we collect from you, or that you provide to us. Where we refer to “Watch”, “we” or “us” in this Privacy Policy, we mean Watch Technology Limited, an Irish company (“Watch Ireland”), and Watch Information Technologies UK Limited (“Watch UK”), a UK company.

If you are between 13 and 18 years old, we have also prepared a separate summary of this policy and what it means for you. It is available in the app under the ‘Privacy Policy’ tab.

SUMMARY

What information do we collect about you?

We collect and process information you give us when you create an account and use the Platform. This includes technical and behavioural information about your use of the Platform. We also collect information about you if you download the app and use the Platform without creating an account.

How will we use the information about you?

We use your information to provide the Platform to you and to improve and administer it. In order to provide an effective and dynamic Platform, and where we have determined it is in our legitimate interests, we use your information to improve and develop the Platform, prevent crime and ensure users’ safety. Where we have your consent, we will also use your personal data to serve you targeted advertising and promote the Platform.

Who do we share your information with?

We share your data with third party service providers who help us to deliver the Platform including cloud storage providers. We also share your information with business partners, other companies in the same group as Watch (including Watch Inc in the US which provides certain services for us in connection with the Platform), content moderation services, measurement providers, advertisers and analytics providers. We may share your information with law enforcement agencies, public authorities or with other third parties only where we are legally required to do so or if such use is reasonably necessary (for instance, to ensure your or someone else’s safety).

Your Rights

We offer you settings to control and manage the personal data we have about you. You also have the following rights: you can ask us to delete your data; to change or correct your data; to provide a copy of your data and to stop using some or all of your data. You can also contact us using the contact information below, and we will review your request in accordance with applicable laws.

How long do we keep hold of your information?

We retain your information for as long as it is necessary to provide you with the service so that we can fulfil our contractual obligations and exercise our rights in relation to the information involved. Where we do not need your information in order to provide the service to you, we retain it only as long as we have a legitimate business purpose in keeping such data or where we are subject to a legal obligation to retain the data. We will also retain your data if necessary for legal claims.

How will we notify you of any changes to this Privacy Policy?

We will notify all users of any material changes to this policy through a notice on our Platform or by other means. We update the “Last Updated” date at the top of this policy, which reflects the effective date of the policy. By accessing or using the Platform, you acknowledge that you have read this policy and that you understand your rights in relation to your personal data and how we will collect, use and process it.

1. The types of personal data we use

We collect and use the following information about you:

Your Profile Information

You give us information when you register on the Platform, including your username, date of birth, email address and/or telephone number, information you disclose in your user profile and your photograph or profile video.

Behavioural Information

We process the content you view on the Platform, including preferences you set (such as choice of language) We collect information through surveys, challenges and competitions in which you participate. We also collect information regarding your use of the Platform, e.g. how you engage with the Platform, including how often you use the Platform and how you interact with content we show you, the ads you view, videos you watch and problems encountered, the content you like, the content you save to “Favourites”, and the words you search.

We infer your interests, gender and age for the purpose of personalising content. We also infer the interests of our users to better optimise advertising across our Platform. If you have consented, we will use this information for the purpose of serving personalised advertising.

We also process information about your followers, the likes you receive and responses to content you upload, for the purposes of personalising your "For You" Feed, promoting your content to other users and exploring whether your profile presents opportunities for collaboration.

Information from Third Parties

You may choose to share certain data with us from third parties or, through your use of the Platform, we may collect such third party data automatically.

Business Partners

If you choose to register to use the Platform using your social media account details (e.g. Facebook, Twitter, Instagram, Google), you will provide us or allow your social network to provide us with your username and public profile. We will likewise share certain information with the relevant social network such as your app ID, access token and the referring URL.

Advertisers and Measurement Partners

Where you have consented to personalised advertising, we will match your information e.g. your mobile advertising ID, where it is provided to us by advertisers and other partners, with your UK Corona Watch profile to serve you ads. We may also serve you ads based on the information we infer from the data these partners provide. You can opt out of this activity at any time via your app settings by going to 'Privacy and safety' and then to 'Personalization and data' and opting out of 'Ads based on data received from partners'.

We use information provided by our measurement partners, to understand how you've interacted with our ad partners' websites and better assess the effectiveness of the advertising on our Platform.

Technical Information we collect about you

We collect certain information from you when you use the Platform including when you are using the app without an account. Such information includes your IP address, instance IDs (which allow us to determine which devices to deliver messages to), mobile carrier, time zone settings, identifier for advertising purposes and the version of the app you are using. We will also collect information regarding the device you are using to access the Platform such as the model of your device, the device system, network type, device ID, your screen resolution and operating system, audio settings and connected audio devices. Where you log-in from multiple devices, we will be able to use your profile information to identify your activity across devices.

Location

When you use the Platform on a mobile device, we will collect information about your location in order to customise your experience. We infer your approximate location based on your IP address. In certain jurisdictions, we may also collect Global Positioning System data.

In-app purchases

If you make in-app purchases, please review our Virtual Items Policy. Your purchase will be made via your Apple iTunes or Google Play account. We do not collect any financial or billing information from you in relation to such a transaction. Please review the relevant app store's terms and notices to learn about how your data is used. We keep a record of the purchases you make, the time at which you make those purchases and the amount spent so that we can credit your account with the correct value in coins.

Information you provide to us

We collect information you provide us in response to a survey. If you respond to a Watch survey, your individual responses will be used for the purpose of the survey and will be shared with other organisations,

as explained to you when you participate in a survey. We may also use aggregate data from these surveys in the same way.

We also collect information you provide to us in correspondence.

Proof of your identity or age

We sometimes ask you to provide proof of identity or age in order to use certain features, such as Livestream or verified accounts, or when you apply for a “Pro Account”.

2. Cookies

Cookies and similar technologies (e.g. pixels and ad tags) (collectively, “**Cookies**”) are small files which, when placed on your device, enable us to collect certain information, including personal data, from you in order to provide certain features and functionality. We and our service providers and business partners use Cookies to collect data and recognise you and your device(s) on the Platform and elsewhere across your different devices. We do this to better understand the effectiveness of the advertising on the Platform and to enhance your user experience.

3. How we use your personal data

We will use the information we collect about you based on the legal grounds described below.

In accordance with, and to perform our contract with you, we will use your information to:

- provide the Platform and associated services;
- notify you about changes to our service;
- provide you with user support;
- enforce our terms, conditions and policies;
- administer the Platform including troubleshooting;
- personalise the content you receive and provide you with tailored content that will be of interest to you;
- enable you to participate in the virtual items program; and
- communicate with you.

In order to comply with our legal obligations and as necessary to perform tasks in the public interest or to protect the vital interests of our users and other people, we use your data to help us prevent and respond to abuse, fraud, illegal activity and other potentially harmful content on the Platform.

In accordance with our legitimate interests to provide an effective and dynamic Platform, we may use your information to:

- ensure your safety and security, including reviewing User Content, messages and associated metadata for breaches of our Community Guidelines and our Terms of Service;
- ensure content is presented in the most effective manner for you and your device;
- understand how people use the Platform so that we can improve, promote and develop it;
- promote popular topics, hashtags and campaigns on the Platform;
- carry out data analysis and test the Platform to ensure its stability and security;
- verify your identity, for example, to enable you to have a 'verified account', and your age, for example, to ensure you are old enough to use certain features;
- provide non-personalised advertising, which keeps many of our services free;
- infer your interests for optimising our advertising offerings, which, where you've consented to personalised advertising, may be based on the information our advertising partners provide to us;
- measure the effectiveness of the advertising you see on our Platform;
- inform our algorithms so we can deliver the most relevant content to you and to prevent crime and misuse of the Platform;
- carry out surveys regarding our services, products and features;
- allow you to participate in interactive features of the Platform; and
- enable you to socialise on the Platform. For example, we may allow other users to identify you via the "Find Friends" function or through their phone contacts or connect you with other users by tracking who you share links with.

Where we process your information to fulfill our legitimate interests, we conduct a balancing test to check that using personal data is really necessary for us to achieve our business purpose. When we carry out this balancing test we also take into account the privacy rights of our users and put in place appropriate safeguards to protect their personal data.

With your consent, we will use your information to provide you with personalised advertising. You can control your personalised advertising settings at any time via your app settings. Please go to 'Privacy and safety' and then 'Personalization and data' to manage and control your advertising preferences. If you do not consent to personalised advertising, you will still see non-personalised advertising on the Platform.

4. How we share your personal data

We share your data with the following selected third parties:

Business Partners

- If you choose to register to use the Platform using your social network account details (e.g. Facebook, Twitter, Instagram, Google), you provide us or allow your social network to provide us with your username and public profile. We will likewise share certain information with the relevant social network such as your app ID, access token and the referring URL.
- Where you opt to share content on social media platforms, username and any text associated with the post will be shared on that platform or, in the case of sharing via instant messaging platforms such as Whatsapp, a link to the content will be shared.

Payment Providers

- If you are 18 or over and choose to buy virtual items we will share data with the relevant payment provider to facilitate this transaction. We share a transaction ID to enable us to identify you and credit your account with the correct value in coins once you have made the payment.

Service Providers

- We provide information and content to service providers who support our business, such as cloud service providers and providers of content moderation services to ensure that the Platform is a safe and enjoyable place.

Analytics and measurement providers

- We use analytics and measurement providers to help us improve the Platform including by assisting us with content measurement and following your activity on our Platform across your devices.
- Our third party analytics and measurement providers also help us measure advertising on our Platform and help our advertisers determine whether their advert has been shown on our Platform and how it performed. We share your mobile advertising ID and other device data with measurement companies so that they can link your activity on the Platform with your activity on our advertisers' websites.

Advertisers

- We only share aggregated user information with advertisers. Aggregated information is information that is grouped together and is not specific to an individual user. This is done to help measure the effectiveness of an advertising campaign by showing advertisers how many users of the Platform have viewed or clicked on an advertisement.

Our Corporate Group

- We may share your information with other members, subsidiaries, or affiliates of our corporate group where it is necessary to provide the Platform in accordance with the Terms of Service.

- We share information to improve and optimise the Platform, including to prevent illegal use and to support users.

Law Enforcement / Legal Obligation

- We may share your information with law enforcement agencies, public authorities or other third parties if we consider that we are legally required to do so or if such use is reasonably necessary to:
 - comply with a legal process or request;
 - enforce our Terms of Service and other agreements, policies, and standards, including investigation of any potential violation;
 - detect, prevent or otherwise address abuse, fraud, illegal activity or security or technical issues; or
 - protect the rights, property or safety of us, our users, a third party or the public as required or permitted by law (including exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction).

Public Profiles

- If your profile is public, your content will be visible to anyone on the Platform and may also be accessed or shared by your friends and followers as well as third parties such as search engines, content aggregators and news sites. You can change who can see a video each time you upload a video. You can also change your profile to private by changing your settings to 'Private account' in 'Privacy and safety' settings. If your profile is public, other users can use your content to produce and upload further content, for example, by creating a duet with your video.

Sale or Merger

- We disclose your information to third parties:
 - in the event that we sell or buy any business or assets (for example, as a result of liquidation, bankruptcy or otherwise). In such transactions, we will disclose your data to the prospective seller or buyer of such business or assets; or
 - if we sell, buy, merge, are acquired by, or partner with other companies or businesses, or sell some or all of our assets. In such transactions, user information may be among the transferred assets.

5. Where we store your personal data

The personal data that we collect from you will be transferred to, and stored at, a destination outside of the European Economic Area ("EEA").

Where we transfer your personal data to countries outside the EEA, we do so under the European Commission's model contracts for the transfer of personal data to third countries (i.e. standard contractual

clauses) pursuant to Commission Decision 2004/915/EC or 2010/87/EU (as appropriate) or in line with any replacement mechanism approved under EU law.

6. Your Rights

We offer you settings to control and manage the personal data we have about you.

You have the following rights:

- **Access Your Data:** You can ask us, free of charge, to confirm we process your personal data and for a copy of your personal data.
- **Delete Your Data:** You can ask us to delete all or some of your personal data.
- **Change or Correct Data:** You can ask us to change or fix your data. You can also make changes using the in-app controls and settings.
- **Portability:** You can ask for a copy of personal data you provided in a machine readable form.
- **Object or Restrict Use of Data and Withdraw Consent:** You can ask us to stop using some or all of your data, e.g. if we have no legal right to keep using it. You can ask us to stop processing your personal data for direct marketing purposes; withdraw your consent or ask us to stop making any automatic individual decisions, including profiling. If you object to such processing, we ask you to share the reason for your objection in order for us to examine the processing of your personal data and to balance our legitimate interest in processing and your objection to this processing.

Before we can respond to a request to exercise one or more of the rights listed above, you may be required to verify your identity or your account details.

For information about how to make these requests, you can contact us using the contact information below, and we will review your request while considering applicable laws. Watch Ireland will be responsible for responding to your request within the relevant periods provided by law. If necessary to resolve your request, Watch Ireland will liaise with Watch UK.

7. The security of your personal data

We take steps to ensure that your information is treated securely and in accordance with this policy. Unfortunately, the transmission of information via the internet is not completely secure. Although we will do our best to protect your personal data, for example, by encryption, we cannot guarantee the security of your information transmitted via the Platform, which means any transmission is at your own risk.

We have appropriate technical and organisational measures to ensure a level of security appropriate to the risk that may be posed to you and other users. We maintain these technical and organisational measures and will amend them from time to time to improve the overall security of our systems.

We will, from time to time, include links to and from the websites of our partner networks, advertisers and affiliates. If you follow a link to any of these websites, please note that these websites have their own privacy policies and that we do not accept any responsibility or liability for these policies. Please check these policies before you submit any information to these websites.

8. How long we keep your personal data

We retain your information for as long as it is necessary to provide you with the service so that we can fulfil our contractual obligations and exercise our rights in relation to the information involved. Where we do not need your information in order to provide the service to you, we retain it only for so long as we have a legitimate business purpose in keeping such data.

If you ask us to delete your account it will first be placed into a deactivated state for 30 days (to allow you to request it to be reinstated), followed by the deletion of the account. We will also delete personal data that relates to the in-app messaging function within 30 days of you cancelling your user account. Please note that messages sent to other users of our service are stored on their devices and cannot be deleted by us.

In each case, there are also occasions where we may need to keep your data for longer in accordance with our legal obligations or where it is necessary for legal claims.

9. Information relating to children

Watch is not directed at children under the age of 13. If you believe that we have personal data about or collected from a child under the relevant age, contact us immediately.

10. Changes

We will notify you of any material changes to this policy through a notice provided via the Platform or by other means. The “Last Updated” date at the top of this policy reflects the effective date of such policy changes.

11. Who we are and how to contact us

Watch Ireland and Watch UK provide the Platform and associated services, and together process personal data in the manner described in this policy and in our Terms of Service. For users of the Platform in the EEA and Switzerland, Watch Ireland is the service provider in accordance with our Terms of Service and if you are in the UK, the provider of the Platform is Watch UK. Watch Ireland and Watch UK share information as joint controllers of your data where it is necessary to do so to operate the Platform efficiently and in line with applicable laws.

CONDITION: PARTIAL POLICY
Privacy Policy

(If you are a user having your usual residence in the US)

Last update: January 1, 2020.

Welcome to Watch (the “Platform”). The Platform is provided and controlled by Watch Inc. (“Watch”, “we” or “us”). We are committed to protecting and respecting your privacy. This Privacy Policy covers the experience we provide for users age 13 and over on our Platform.

Capitalized terms that are not defined in this policy have the meaning given to them in the Terms of Service.

SUMMARY

What information do we collect about you?

We collect and process information you give us when you create an account and use the Platform. This includes technical and behavioural information about your use of the Platform. We also collect information about you if you download the app and use the Platform without creating an account.

How will we use the information about you?

We use your information to provide the Platform to you and to improve and administer it. In order to provide an effective and dynamic Platform, and where we have determined it is in our legitimate interests, we use your information to improve and develop the Platform, prevent crime and ensure users’ safety. Where we have your consent, we will also use your personal data to serve you targeted advertising and promote the Platform.

Who do we share your information with?

We share your data with third party service providers who help us to deliver the Platform including cloud storage providers. We also share your information with business partners, other companies in the same group as Watch (including Watch Inc in the US which provides certain services for us in connection with the Platform), content moderation services, measurement providers, advertisers and analytics providers. We may share your information with law enforcement agencies, public authorities or with other third parties only where we are legally required to do so or if such use is reasonably necessary (for instance, to ensure your or someone else’s safety).

Your Rights

We offer you settings to control and manage the personal data we have about you. You also have the following rights: you can ask us to delete your data; to change or correct your data; to provide a copy of your data and to stop using some or all of your data. You can also contact us using the contact information below, and we will review your request in accordance with applicable laws.

How long do we keep hold of your information?

We retain your information for as long as it is necessary to provide you with the service so that we can fulfil our contractual obligations and exercise our rights in relation to the information involved. Where we do not need your information in order to provide the service to you, we retain it only as long as we have a legitimate business purpose in keeping such data or where we are subject to a legal obligation to retain the data. We will also retain your data if necessary for legal claims.

How will we notify you of any changes to this Privacy Policy?

We will notify all users of any material changes to this policy through a notice on our Platform or by other means. We update the “Last Updated” date at the top of this policy, which reflects the effective date of the policy. By accessing or using the Platform, you acknowledge that you have read this policy and that you understand your rights in relation to your personal data and how we will collect, use and process it.

For more information, click [here](#).

CONDITION: PICTURE

Note: Images found on Pixabay, Free Use

Privacy Policy

(If you are a user having your usual residence in the US)

Last update: January 1, 2020.

Welcome to Watch (the “Platform”). The Platform is provided and controlled by UK Corona Watch Inc. (“Watch”, “we” or “us”). We are committed to protecting and respecting your privacy. This Privacy Policy covers the experience we provide for users age 13 and over on our Platform.

Capitalized terms that are not defined in this policy have the meaning given to them in the Terms of Service.

SUMMARY

What information do we collect about you?

We collect and process information you give us when you create an account and use the Platform. This includes technical and behavioural information about your use of the Platform. We also collect information about you if you download the app and use the Platform without creating an account.



How will we use the information about you?

We use your information to provide the Platform to you and to improve and administer it. In order to provide an effective and dynamic Platform, and where we have determined it is in our legitimate interests, we use your information to improve and develop the Platform, prevent crime and ensure users' safety. Where we have your consent, we will also use your personal data to serve you targeted advertising and promote the Platform.



Who do we share your information with?

We share your data with third party service providers who help us to deliver the Platform including cloud storage providers. We also share your information with business partners, other companies in the same group as Watch (including Watch Inc in the US which provides certain services for us in connection with the Platform), content moderation services, measurement providers, advertisers and analytics providers. We may share your information with law enforcement agencies, public authorities or with other third parties only where we are legally required to do so or if such use is reasonably necessary (for instance, to ensure your or someone else's safety).

Your Rights

We offer you settings to control and manage the personal data we have about you. You also have the following rights: you can ask us to delete your data; to change or correct your data; to provide a copy of your data and to stop using some or all of your data. You can also contact us using the contact information below, and we will review your request in accordance with applicable laws.

How long do we keep hold of your information?

We retain your information for as long as it is necessary to provide you with the service so that we can fulfil our contractual obligations and exercise our rights in relation to the information involved. Where we do not need your information in order to provide the service to you, we retain it only as long as we have a legitimate business purpose in keeping such data or where we are subject to a legal obligation to retain the data. We will also retain your data if necessary for legal claims.



How will we notify you of any changes to this Privacy Policy?

We will notify all users of any material changes to this policy through a notice on our Platform or by other means. We update the “Last Updated” date at the top of this policy, which reflects the effective date of the policy. By accessing or using the Platform, you acknowledge that you have read this policy and that you understand your rights in relation to your personal data and how we will collect, use and process it.

For more information, click [here](#).

REFERENCES

- 6, P. (1998). *The future of privacy, volume 1: Private life and public policy*. Demos, London, UK.
- 6, P., Lasky, K., & Fletcher, A. (1998). *The future of privacy, volume 2: Public trust and the use of private information*. Demos, London, UK.
- Adey, P. (2006). "Divided we move": The dromologies of airport security and surveillance. In T. Monahan (Ed.), *Surveillance and security: Technological politics and power in everyday life* (pp. 195-208). New York, NY: Routledge.
- Aguirre, E., Mahr, D., Grewal, D., de Yuyter, K., & Wetzels, M. (2015). Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness. *Journal of Retailing*, 91, 34-49.
- Aladwani, A. M. (2017). Compatible quality of social media content: Conceptualization, measurement, and affordance. *International Journal of Information Management*, 37, 576-582.
- Aldhafferi, N., Watson, C., & Sajeev, A. S. M. (2013). Personal information privacy settings of online social networks and their suitability for mobile Internet devices. *International Journal of Security, Privacy, and Trust Management*, 2(2), 1-17.
- Altman, I. (1975). *The environment and social behavior*. Monterey, CA: Brooks/Cole.
- Altman, I. (1977). Privacy regulation: Culturally universal or culturally specific? *Journal of Social Issues*, 33(3), 66-84. doi:10.1111/j.1540-4560.1977.tb01883.x
- Ampong, G. O. A., Mensah, A., Adu, A. S. Y., Addae, J. A., Omoregie, O. K., & Ofori, K. S. (2018). Examining self-disclosure on social networking sites: A flow theory and privacy perspective. *Behavioral Sciences*, 8(58), 1-17.

- Areepattamannil, S., & Khine, M. S. (2017). Early adolescents' use of information and communication technologies (ICTs) for social communication in 20 countries: Examining the roles of ICT-related behavioral and motivational characteristics. *Computers in Human Behavior*, 73, 263-272.
- Angulo, J., Fischer-Hübner, S., Wästlund, E., & Pulls, T. (2012). Towards usable privacy policy display and management. *Information Management & Computer Security*, 20, 4-17. doi:10.1108/09685221211219155
- Badshah, N. (2018, April 8). Facebook to contact 87 million users affected by data breach. *The Guardian*. Retrieved from <https://www.theguardian.com/technology/2018/apr/08/facebook-to-contact-the-87-million-users-affected-by-data-breach>
- Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, 11, 1-12. Retrieved from <http://firstmonday.org/ojs/index.php/fm/article/view/1394/1312>
- Bernard, R., Bowsher, G., Milner, C., Boyle, P., Patel, P., & Sullivan, R. (2018). Intelligence and global health: Assessing the role of open source and social media intelligence analysis in infectious disease outbreaks. *Journal of Public Health*, 26, 509-514. doi:10.1007/s10389-018-0899-3
- Bernstein, G. (2006). The paradoxes of technological diffusion: Genetic discrimination and Internet privacy. *Connecticut Law Review*, 39, 241-296.
- Bhatia, J., & Breaux, T. D. (2018). Semantic incompleteness in privacy policy goals. Paper presented at 2018 IEEE 26th International Requirements Engineering Conference, Banff, Canada. doi:10.1109/RE.2018.00025

- Bowman, N. D., Westerman, D. K., & Claus, C. J. (2012). How demanding is social media: Understanding social media diets as a function of perceived costs and benefits – A rational actor perspective. *Computers in Human Behaviors*, 28(6), 2295-2305. doi:10.1016/j.chb.2012.06.037
- Bradford, A. (2018, April 24). Everything you need to master Instagram Stories. CNET. Retrieved from <https://www.cnet.com/how-to/how-to-use-instagram-stories/>
- Bragg, M. A., Miller, A. N., Kalkstein, D. A., Elbel, B., & Roberto, C. A. (2019). Evaluating the influence of racially targeted food and beverage advertisements on Black and White adolescents' perceptions and preferences. *Appetite*, 140, 41-49.
- Brandtzaeg, P. B. (2010). Towards a unified media-user typology (MUT): A meta-analysis and review of the research literature on media-user typologies. *Computers in Human Behavior*, 26, 940-956.
- Brown, R. (2020, July 03). Why coronavirus contact-tracing apps aren't the 'game changer' authorities hoped they'd be. CNBC. Retrieved from <https://www.cnbc.com/2020/07/03/why-coronavirus-contact-tracing-apps-havent-been-a-game-changer.html>
- Byford, S. (2020, June 19). Japan rolls out Microsoft-developed COVID-19 contact tracing app. *The Verge*. Retrieved from <https://www.theverge.com/2020/6/19/21296603/japan-covid-19-contact-tracking-app-cocoa-released>
- Caluya, G. (2010). The post-panoptic society? Reassessing Foucault in surveillance studies. *Social Identities*, 16(5), 621-633. doi:10.1080/13504630.2010.509565

- Cheung, C., Bietz, M. J., Patrick, K., & Bloss, C. S. (2016). Privacy attitudes among early adopters of emerging health technologies. *PLoS ONE*, 11(11): e0166389, 1-12. doi:10.1371/journal.pone.0166389
- Child, J. T., & Westermann, D. A. (2013). Let's be Facebook friends: Exploring parental Facebook friend requests from a communication privacy management (CPM) perspective. *Journal of Family Communication*, 13, 46-59. doi:10.1080/15267431.2012.742089
- Cho, E., Sundar, S. S., Abdullah, S., & Motalebi, N. (2020). Will deleting history make Alexa more trustworthy? Effects of privacy and content customization on user experience of smart speakers. Paper presented at the 2020 CHI Conference on Human Factors in Computing Systems, Honolulu, HI, USA. doi:10.1145/3313831.3376551
- Choi, Y. H., & Bazarova, N. N. (2015). Self-disclosure characteristics and motivations in social media: Extending the functional model to multiple social network sites. *Human Communication Research*, 41, 480-500. doi:10.1111/hcre.12053
- Craig, R. T. (1996). Practical theory: A reply to Sandelands. *Journal for the Theory of Social Behavior*, 26(1), 65-79.
- Craig, R. T. (1999). Communication theory as a field. *Communication Theory*, 9(2), 119-161.
- Crano, W. D., Alvaro, E. M., Tan, C. N., & Siegel, J. T. (2017). Social mediation of persuasive media in adolescent substance prevention. *Psychology of Addictive Behaviors*, 31(4), 479-487.

- Crosman, P. (2020, July 13). Lawsuit against Plaid heightens focus on data privacy issues. *American Banker*. Retrieved from <https://www.americanbanker.com/news/lawsuit-against-plaid-heightens-focus-on-data-privacy-issues>
- Culp, S. (2016, May 10). Cyber risk: People are often the weakest link in the security chain. *Forbes*. Retrieved from <https://www.forbes.com/sites/steveculp/2016/05/10/cyber-risk-people-are-often-the-weakest-link-in-the-security-chain/#359e92d22167>
- David, K., & James, C. (2013). Tweens' conceptions of privacy online: Implications for educators. *Learning, Media, & Technology*, 38(1), 4-25.
doi:10.1080/17439884.2012.658404
- Delfino, D. (2019, August 15). How to make a private story on Snapchat that can only be seen by the friends you choose. *Business Insider*. Retrieved from <https://www.businessinsider.com/how-to-make-a-private-story-on-snapchat>
- Dev, J. (2020). Discussing privacy and surveillance on Twitter: A case study of COVID-19. arXiv. doi: 10.13140.RG.2.2.14162.38083
- Dinev, T., & Hart, P. (2005). Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce*, 10(2), 7-29.
- Doffman, Z. (2020a, August 08). Why you should stop sending SMS messages – even on Apple iMessage. *Forbes*. Retrieved from <https://www.forbes.com/sites/zakdoffman/2020/08/08/apple-iphone-ipad->

imessage-security-update-sms-rcs-google-whatsapp-
encryption/?sh=7fd028495b4d

Doffman, Z. (2020b, August 13). Why you must beware what you ask Amazon Alexa.

Forbes. Retrieved from

<https://www.forbes.com/sites/zakdoffman/2020/08/13/amazon-alexa-cyber-attack-check-point-report-smart-speaker-warning/#28727e8a5008>

Ellison, N. B., Gibbs, J. L., & Weber, M. S. (2015). The use of enterprise social network

sites for knowledge sharing in distributed organizations: The role of

organizational affordances. *American Behavioral Scientist*, 59, 103-123.

doi:10.1177/0002764214540510

Ellison, N. B., Vitak, J., Steinfield, C., Gray, R., & Lampe, C. (2011). Negotiating

privacy concerns and social capital needs in a social media environment. In

Privacy online (pp. 19-32). Springer, Berlin, Heidelberg.

English, P. (2016). Twitter's diffusion in sports journalism: Role models, laggards and

followers of the social media innovation. *New Media & Society*, 18(3), 484-501.

doi:10.1177/1461444814544886

Evans, S. K., Pearce, K. E., Vitak, J., & Treem, J. W. (2017). Explicating affordances: A

conceptual framework for understanding affordances in communication research.

Journal of Computer-Mediated Communication, 22, 35-52.

Feibus, M. (2020, June 24). Are coronavirus contact tracing apps doomed to fail in

America? USA Today. Retrieved from

<https://www.usatoday.com/story/tech/columnist/2020/06/24/apple-google-contact-tracing-apps-privacy/3253088001/>

- Fox, J., & Potocki, B. (2014). Technology and culture: Sociocultural explanations for sexting. In T. C. Heistand & W. J. Weins (Eds.), *Sexting and youth: A multidisciplinary examination of research, theory, and law* (pp. 95-112). Durham: Carolina Academic Press.
- Fowler, G. A. (2020, July 13). Is it time to delete TikTok? A guide to the rumors and privacy risks. *The Washington Post*. Retrieved from <https://www.washingtonpost.com/technology/2020/07/13/tiktok-privacy/>
- Feyerabend, P. (1983). How to defend society against science. In I. Hacking (Ed.), *Scientific Revolutions* (pp. 156-167). Oxford, England: Oxford University Press.
- General Data Protection Regulation (GDPR). (2016). *Official Journal of the European Union*, 119, 1-88. Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>
- Gibson, J. J. (1977). The theory of affordances. In R. Shaw and J. Bransford (Ed.), *Perceiving, acting, knowing* (pp. 67-82). Lawrence Erlbaum.
- Gibson, J. J. (1986). *The ecological approach to visual perception*. Houghton Mifflin.
- Grier, S. A., & Kumanyika, S. (2010). Targeted marketing and public health. *Annual Review of Public Health*, 31, 349-369.
- Hargittai, E., & Marwick, A. (2016). “What can I really do?” Explaining the privacy paradox with online apathy. *International Journal of Communication*, 10, 3737-3757.
- Harwell, D. (2019, December 24). Colleges are turning students’ phones into surveillance machines, tracking the locations of hundreds of thousands. *The Washington Post*. Retrieved from

<https://www.washingtonpost.com/technology/2019/12/24/colleges-are-turning-students-phones-into-surveillance-machines-tracking-locations-hundreds-thousands/>

Hesse, B. (2020, December 09). How to enable end-to-end encryption in Google Messages. Lifehacker. Retrieved from <https://lifehacker.com/how-to-enable-end-to-end-encryption-in-google-messages-1845845418>

Jeong, S. (2018, May 22). No one's ready for GDPR. The Verge. Retrieved from <https://www.theverge.com/2018/5/22/17378688/gdpr-general-data-protection-regulation-eu>

Johnson, J. P. (2013). Targeted advertising and advertising avoidance. *RAND Journal of Economics*, 44(1), 128-144.

Karahanna, E., Xu, S. X., Xu, Y., & Zhang, N. (2018). The needs-affordances-features perspective for the use of social media. *MIS Quarterly*, 42(3), 737-756.

Katulić, T., & Katulić, A. (2018). GDPR and the reuse of personal data in scientific research. Paper presented at MIPRO 2018: 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia.

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

- Kim, T., Barasz, K., & John, L. K. (2019). Why am I seeing this ad? The effect of ad transparency on ad effectiveness. *Journal of Consumer Behavior Research*, 45, 906-932.
- Kizza, J., & Ssanyu, J. (2005). Workplace surveillance. In J. Weckert (ed.), *Electronic monitoring in the workplace. Controversies and solutions* (pp. 1-18). London: Idea Group Publishing.
- Koohang, A. (2017). Social media sites privacy concerns: Empirical validation of an instrument. *Online Journal of Applied Knowledge Management*, 5(1), 14-26.
- Koskela, H. (2004). Webcams, TV shows and mobile phones: Empowering exhibitionism. *Surveillance & Society*, 2(2/3), 199-215.
- Koskela, H. (2009). Hijacking surveillance? The new moral landscapes of amateur photographing. In K. F. Aas, H. O. Gundhus, & H. M. Lomell (Eds.), *The surveillance of everyday life* (pp. 147-167). New York, NY: Routledge-Cavendish.
- Kox, H., Straathof, B., & Zwart, G. (2017). Targeted advertising, platform competition, and privacy. *Journal of Economics and Management Strategy*, 26, 557-570.
- Krasnova, H., Günther, O., Spiekermann, S., & Koroleva, K. (2009). Privacy concerns and identity in online social networks. *IDIS*, 2, 39-63.
- Lim, V. K. G. (2002). The IT way of loafing on the job: Cyberloafing, neutralizing, and organizational justice. *Journal of Organizational Behavior*, 23(5), 675-694.
- Littlejohn, S. W. (2009). Evaluating communication theory. In S. W. Littlejohn & K. A. Foss (Eds.), *Encyclopedia of communication theory*, Vol. 1 (pp. 363-365). Thousand Oaks, CA: Sage.

- Livingstone, S. (2008). Taking risky opportunities in youthful content creation: Teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media & Society*, 10, 393-411. doi:10.1177/1461444808089415
- Lyon, D. (2010). Surveillance, power, and everyday life. In P. Kalantzis-Cope & K. Gherabe-Martin (Eds.), *Emerging digital spaces in contemporary society* (pp. 107-120). Houndsmills, UK: Palgrave Macmillan.
- MacKinnon, R. (2012). *Consent of the networked*. New York, NY: Basic Books.
- Malala, J. (2016). Communication privacy management and the digital footprint in pervasive computer-mediated communication. *International Journal of Advanced Research in Computer Science*, 7(7), 31-41.
- Margulis, S. T. (1977). Conceptions of privacy: Current status and next steps. *Journal of Social Issues*, 33(3), 5-21. doi:10.1111/j.1540-4560.1977/tb01879
- Margulis, S. T. (2003). On the status and contribution of Westin's and Altman's theories of privacy. *Journal of Social Issues*, 59(2), 411-429. doi:10.1111/1540-4560.00071
- Martin, A. J., Wellen, J. M., & Grimmer, M. R. (2016). An eye on your work: How empowerment affects the relationship between electronic surveillance and counterproductive work behaviors. *The International Journal of Human Resource Management*, 27(21), 2635-3651. doi:10.1080/09585192.2016.1225313
- Mayeda, G. (2016). Privacy in the age of the Internet: Lawful access provisions and access to ISP and OSP subscriber information. *Alberta Law Review*, 53(3), 709-746.

- Meier, Y., Schäwel, J., & Krämer, N. C. (2020). The shorter the better? Effects of privacy policy length on online privacy decision-making. *Media and Communication*, 8(2), 291-301. doi:10.17645/mac.v8i2.2846
- Metzger, M. J. (2007). Communication privacy management in electronic commerce. *Journal of Computer-Mediated Communication*, 12, 335-361. doi:10.1111/j.1083-6101.2007.00328
- Miller, F., Davis, K., & Partridge, H. (2019). Everyday life information experiences in Twitter: A grounded theory. *Information Research*, 24(2), 1-32.
- Monahan, T. (2011). Surveillance as cultural practice. *The Sociological Quarterly*, 52(4), 495-508.
- Montieri, A., Ciunzo, D., Aceto, G., & Pescapé, A. (2017). Anonymity services Tor, I2P, JonDonym: Classifying in the dark. Paper presented at the 29th International Teletraffic Congress (ITC 29), Genoa, Italy.
- Mujtaba, B. G. (2003). Ethical implications of employee monitoring: What leaders should consider. *Journal of Applied Management and Entrepreneurship*, 8(3), 22-47.
- Nye, B. D., & Silverman, B. G. (2012). Affordance. In N. M. Seel (Ed.), *Encyclopedia of the sciences of learning* (pp. 179-183). New York, NY: Springer.
- Papacharissi, Z. (2010). Privacy as a luxury commodity. *First Monday*, 15(8). Retrieved from <http://firstmonday.org/ojs/index.php/fm/article/view/3075/2581-09-29>
- Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. Albany, NY: State University of New York Press.

- Petronio, S. (2013). Brief status report on communication privacy management theory. *Journal of Family Communication*, 13, 6-14.
- Ploug, T., & Holm, S. (2013). Informed consent and routinisation. *Journal of Medical Ethics*, 39(4), 214-218. doi:10.1136/medethics-2012-101056
- Pollach, I. (2005). A typology of communicative strategies in online privacy policies: Ethics, power, and informed consent. *Journal of Business Ethics*, 62, 221-235. doi:10.1007/s10551-005-7898-3
- Quinn, K. (2016). Why we share: A uses and gratifications approach to privacy regulation in social media use. *Journal of Broadcasting & Electronic Media*, 60(1), 61-86. doi:10.1080/08838151.2015.112745
- Rathnayake, C., & Winter, J. S. (2018). Carrying forward the uses and grats 2.0 agenda: An affordance-driven measure of social media uses and gratifications. *Journal of Broadcasting & Electronic Media*, 62(3), 371-389.
- Rice, R. E., Evans, S. K., Pearce, K. E., Sivunen, A., Vitak J., & Treem, J. W. (2017). Organizational media affordances: Operationalization and associations with media use. *Journal of Communication*, 67, 106-130.
- Rogers, E. M. (1962). *Diffusion of innovations*. New York, NY: Free Press.
- Rossi, A., & Palmirani, M. (2017). A visualization approach for adaptive consent in the European Data Protection Framework. Paper presented at 2017 International Conference for E-Democracy and Open Government (CeDEM), Krems, Austria. doi:10.1109/CeDEM.2017.23

- Rulffes, A. M. (2017). Privacy vs. security: Fear appeals, terrorism, and the willingness to allow increased government surveillance (Doctoral dissertation). Available from ProQuest Dissertations and Theses A&I Database. (UMI No. 10270691).
- Sandelands, L. E. (1990). What is so practical about theory? Lewin revisited. *Journal for the Theory of Social Behavior*, 20, 235-262.
- Santos, M., & Faure, A. (2018). Affordance is power: Contradictions between communicational and technical dimensions of WhatsApp's end-to-end encryption. *Social Media + Society*, 4(3), 1-16.
- Sarabdeen, J., & Moonesar, I. A. (2018). Privacy protection laws and public perception of data privacy. *Benchmarking: An International Journal*, 25(6), 1883-1902.
- Sayre, G. M., & Dahling, J. J. (2016). Surveillance 2.0: How personality qualifies reactions to social media monitoring policies. *Personality and Individual Differences*, 90, 254-259. doi:10.1016/j.paid.2015.11.021
- Schrock, A. R. (2015). Communicative affordances of mobile media: Portability, availability, locatability, and multimediality. *International Journal of Communication*, 9, 1229-1246.
- Schwartz, J., & Grimm, J. (2017). PrEP on Twitter: Information, barriers, and stigma. *Health Communication*, 32(4), 509-516. doi:10.1080/10410236.2016.1140271
- Schwarz, J. (2020, February 10). How much privacy are students surrendering to attendance-tracking app? The Hill. Retrieved from <https://thehill.com/opinion/cybersecurity/482282-how-much-privacy-are-students-surrendering-to-attendance-tracking-app>

- Shilton, K. (2009). Four billion little brothers? Privacy, mobile phones, and ubiquitous data collection. *Communications of the ACM*, 52(11), 48-53.
- Shin, W., Huh, J., & Faber, R. J. (2012). Tweens' online privacy risks and the role of parental mediation. *Journal of Broadcasting & Electronic Media*, 56(4), 632-649. doi:10.1080/08838151.2012.732135
- Shreeves, M. (2015). Risk processing, affect, and efficacy in online privacy behavior (Master's thesis). Available from ProQuest Dissertations and Theses A&I Database. (UMI No. 1597074).
- Siegert, S., & Löwstedt, J. (2019). Online boundary work tactics: An affordance perspective. *New Technology, Work and Employment*, 34, 18-36.
- Sirota, D. (2019). California's new data privacy law brings U.S. closer to GDPR. TechCrunch. Retrieved from <https://techcrunch.com/2019/11/14/californias-new-data-privacy-law-brings-u-s-closer-to-gdpr/>
- Steuber, K. R., & Solomon, D. H. (2012). Relational uncertainty, partner interference, and privacy boundary turbulence: Explaining spousal discrepancies in infertility disclosures. *Journal of Social and Personal Relationships*, 29(1), 3-27. doi:10.1177/0265407511406896
- Such, J. M., & Rovatsos, M. (2016). Privacy policy negotiation in social media. *ACM Transactions on Autonomous and Adaptive Systems*, 11(1): 4.2-4.28.
- Sundar, S. S. (2008). The MAIN model: A heuristic approach to understanding technology effects on credibility. In M. J. Metzger & A. J. Flanagin (Eds.), *Digital media, youth, and credibility* (pp. 73-100). Cambridge, MA: The MIT Press.

- Sundar, S. S., Kang, H., Zhang, B., Go, E., & Wu, M. (2013). Unlocking the privacy paradox: Do cognitive heuristics hold the key? Poster presented at the 31st Annual CHI Conference on Human Factors in Computing Systems, Paris, France.
doi:10.1145/2468356.2468501
- Sundar, S. S., & Limperos, A. M. (2013). Uses and Grats 2.0: New gratifications for new media. *Journal of Broadcasting & Electronic Media*, 57(4), 504-525.
- Sundar, S. S., & Marathe, S. S. (2010). Personalization versus customization: The importance of agency, privacy, and power usage. *Human Communication Research*, 36, 298-322. doi:10.1111/j.1468-2958.2010.01377.x
- Treem, J. W., & Leonardi, P. M. (2012). Social media use in organizations. *Communication Yearbook*, 36, 143-189. doi:10.2139/ssrn.2129853
- Vorderer, P. (2016). Communication and the good life: Why and how our discipline should make a difference. *Journal of Communication*, 68, 1-12.
- Wakefield, J. (2019, November 14). Social-media influencers: Incomes soar amid growing popularity. BBC. Retrieved from
<https://www.bbc.com/news/technology-50418807>
- Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 4(5), 193-220.
- Westin, A. (1967). *Privacy and freedom*. New York: Atheneum.
- White, M. D., & Marsh, E. E. (2006). Content analysis: A flexible methodology. *Library Trends*, 55(1), 22-45. <http://dx.doi.org/10.1353/lib.2006.0053>
- Woodruff, A., & Aoki, P. M. (2004). Push-to-talk social talk. *Computer Supported Cooperative Work (CSCW)*, 13, 409-441.

- Xu, H., Gupta, S., Rosson, M. B., & Carroll, J. M. (2012). Measuring mobile users' concerns for information privacy. Paper presented at the 33rd International Conference on Information Systems, Orlando, FL, USA.
- Yang, C.-C. (2018). Social media as more than a peer space: College freshmen encountering their parents on Facebook. *Journal of Adolescent Research*, 33(4), 442-469. doi:10.1177/0743558416659750
- Yuan, E. J., Feng, M., & Danowski, J. A. (2013). "Privacy" in semantic networks on Chinese social media: The case of Sina Weibo. *Journal of Communication*, 63, 1011-1031. doi:10.1111/jcom.12058
- Youn, T., Kim, J., & Lim, M. (2014). Study on two privacy-oriented protocols for Information Communication Systems. *Journal of Intelligence Manufacturing*, 25, 339-345.
- Zajko, M. (2018). Internet Service Providers as privacy custodians. *Canadian Journal of Law and Society*, 33(3), 401-423.
- Zhou, T. (2017). Understanding location-based services users' privacy concern: An elaboration likelihood model perspective. *Internet Research*, 27(3), 506-519. doi:10.1108/IntR-04-2016-0088

VITA

EDUCATION

M.A., Communication (May 2017), San Diego State University

Thesis: The Threads of Threat Analysis: Natural Language and the Perception of Threat Seriousness

Advisor: Dr. Brian H. Spitzberg

Committee: Dr. Rachael A. Record & Dr. Jean M. Gawron

B.A., Speech Communications (May, 2014), University of La Verne

Major in Speech Communications, *Minor* in Software

ACADEMIC AND PROFESSIONAL APPOINTMENTS

- Aug 2017-Present *Doctoral Graduate Teaching Assistant*, Department of Communication, College of Communication and Information, University of Kentucky
- Dec 2016-Present *Parliamentarian*, United States Universities Debating Association
- Aug 2015-Aug 2017 *Graduate Teaching Assistant*, School of Communication, College of Professional Studies & Fine Arts, San Diego State University
- Aug 2015-Aug 2017 *Forensics Administrator*, School of Communication, College of Professional Studies & Fine Arts, San Diego State University

HONORS/AWARDS

- 2020 Martha and Howard Sypher Memorial Graduate Scholarship, University of Kentucky (\$1,000)
- 2020 Em Griffin Top (Student) Paper Award, Communication Theory Interest Group, Central States Communication Association (CSCA)
- 2019 Dorothy M. Carozza Memorial Fellowship Fund, University of Kentucky (\$1,000)
- 2018 Dorothy M. Carozza Memorial Fellowship Fund, University of Kentucky (\$1,000)
- 2017 Outstanding Graduate Student, San Diego State University School of Communication

- 2016 NCA Caucus Student Travel Grant (LGBTQ Concerns), National Communication Association (\$200)
- 2016 Gracia Mae Ogden Memorial Scholarship, San Diego State of University (\$700)
- 2016 Graduate Equity Fellowship, San Diego State University (\$1,000)
- 2015 Graduate Equity Fellowship, San Diego State University (\$1,000)
- 2015 Sarah Steltzer Scholarship for Study Abroad, San Diego State University (\$500)
- 2014 Dean's Award for Senior Project – Excellence in Research, Social Science Division, University of La Verne (\$250)
- 2014 Dr. Jeanne Flora Award Finalist, Speech Communications Department, University of La Verne
- 2014 Institutional Honors – Cum Laude, University of La Verne

PUBLISHED MANUSCRIPTS AT REFEREED JOURNALS

3. Ivanov, B., Hester, E., Martin, J., **Silberman, W.**, Slone, A., Goatley-Soan, S., Geegan, S., Parker, K. A., Herrington, T., Riker, S., & Anderson, A. (accepted). Persistence of emotion in the process of inoculation: Experiencing post-attack threat, fear, anger, happiness, sadness, and surprise. *Communication Quarterly*.
2. Parker, K. A., Geegan, S., Ivanov, B., Slone, A., **Silberman, W.**, Martin, J., . . . Riker, S. (2019). Defending democracy: Inoculation's efficacy in protecting First Amendment attitudes. *Communication Studies*, 71(1), 22-39.
<https://doi.org/10.1080/10510974.2019.1671889>
1. Record, R. A., **Silberman, W. R.**, Santiago, J., & Ham, T. (2018). I sought it, I *Reddit*: Examining health information engagement behaviors among *Reddit* users. *Journal of Health Communication*, 23(5), 470-476.
<http://dx.doi.org/10.1080/10810730.2018.1465493>

INVITED BOOK CHAPTERS

1. Limperos, A. M., & **Silberman, W. R.** (2019). Agenda setting in the age of emergent online media and social networks: Exploring the dangers of a news agenda influenced by subversive and fake information. In E. Downs (Ed.), *Dark side of media & technology* (pp. 37-48). Peter Lang: Switzerland.

COMPETITIVE CONFERENCE PAPER/POSTER/PANEL PRESENTATIONS

17. **Silberman, W. R.**, & Record, R. A. (2021, May). *We post it, U Reddit: Exploring the potential of Reddit for health interventions targeting college populations*. Paper to be presented at the International Communication Association, Communication & Technology Division. *Virtual Convention*.
16. **Silberman, W. R.**, Limperos, A., & Lewis, N. (2020, November). *Islands in the (Live)Stream: Understanding the Relationship between Public and Private Gaming*. Paper presented at the National Communication Association, Game Studies Division, *Virtual Convention*.
15. **Silberman, W. R.** (2020, April). *Mediated modern privacy: A theoretical review*. **Top Student Paper** presented at the Central States Communication Association, Communication Theory Division, Chicago, IL.
14. **Silberman, W. R.**, Steinberg, D., Dhillon, K., Ruiz, R., Margesson, R., Iberri-Shea, G., & Aranda, N. (2020, April). *Best practices in British Parliamentary debate tournament management*. Panel presented at the Central States Communication Association, Argumentation and Forensics Division, Chicago, IL.
13. Ivanov, B., Martin, J., Hester, E., **Silberman, W. R.**, Slone, A., Goatley-Soan, S., . . . Anderson, A. (2019, November). *Post-inoculation attack: Experiencing threat, fear, anger, happiness, sadness, and surprise*. Paper presented at the National Communication Association, Baltimore, MD
12. Parker, K., Ivanov, B., Geegan, S., Slone, A., **Silberman, W. R.**, Martin, J., . . . Riker, S. (2019, May). *Defending democracy: Inoculation's efficacy in protecting First Amendment attitudes*. Poster presented at the International Communication Association, Information Systems Interactive Poster Session: Washington, D.C., USA.
11. Sutton, J., Studts, J., & **Silberman, W. R.** (2018, April). *Lung cancer screening awareness: The thoughts and beliefs of family and friends of individuals at risk for developing lung cancer*. Poster presented at the Kentucky Conference on Health Communication, Cancer-Focused Health Communication Research Session: Lexington, KY.
10. **Silberman, W. R.**, & Spitzberg, B. H. (2017, November). *THREADing the needle: Modeling a big data approach to threat message identification and assessment*. Paper presented at the National Communication Association, Interpersonal Communication Division: Dallas, TX.
9. **Silberman, W. R.** (2017, November). *Sure, you won, but you can still improve: Encouraging adjudication to feature reasons for decision and room for improvement*. Paper presented at the National Communication Association, American Forensic Association Panel: Dallas, TX.

8. **Silberman, W. R.** (2017, November). *Guilty confessions of a Jew-ish son: An autoethnographic account from one wandering Jew to another*. Paper presented at the National Communication Association, Ethnography Division: Dallas, TX.
7. **Silberman, W. R.**, Kaiser, E., & Spitzberg, B. H. (2017, November). *Are stalkers crazy, mean, or both?: A meta-analysis on mental disorders, violence, and stalking*. Paper presented at the National Communication Association, Interpersonal Communication Division: Dallas, TX.
6. **Silberman, W. R.**, Santiago, J., & Ham, T. (2017, March). *I sought it, I Reddit: Examining health information seeking behaviors among Reddit users*. Paper presented at the SDSU Research Symposium. San Diego, CA.
5. **Silberman, W. R.**, Record, R. A., Santiago, J., & Ham, T. (2017, May). *I sought it, I Reddit: Examining health information seeking behaviors among Reddit users*. Paper presented at the Partnership for Progress on the Digital Divide 2017 International Conference: San Diego, CA.
4. **Silberman, W. R.** (2017, February). *Guilt(y) appeals within guilty memorials: A critique of the Dachau Memorial site*. Paper presented at the Western States Communication Association Conference, Rhetoric and Public Address Division: Salt Lake City, UT.
3. Martinez, L., Record, R.A., **Silberman, W. R.**, Kaiser, E., & Wehlage, S. (2016, November). *Run the risk or take a chance? Comparing effects of probabilistic frames on behavioral intention*. Paper presented at the National Communication Association Conference, Applied Communication Division: Philadelphia, PA.
2. Record, R. A., Ham, T., **Silberman, W. R.**, Majmundar, A., & Bowe, K. (2016, November). *Yik Yak as an intervention platform: Assessing the usability of Yik Yak for health interventions*. Paper presented at the National Communication Association Conference, Human Communication and Technology Division: Philadelphia, PA.
1. **Silberman, W. R.** (2016, November). *Memoirs of a gay son: Attempting to pass the performative test of heteronormativity*. Paper presented at the National Communication Association Conference, Ethnography Division: Philadelphia, PA.